HP StorageWorks

Fabric OS 5.x Advanced Web Tools administrator guide

Part number: AA–RVHYB–TE
Second edition: September 2005

Legal and notice information

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information is provided "as is" without warranty of any kind and is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Windows and Windows XP are U.S. registered trademarks of Microsoft Corporation.

UNIX is a registered trademark of The Open Group.

Linux is a U.S. registered trademark of Linus Torvalds.

Java is a U.S. trademark of Sun Microsystems, Inc.

Fabric OS 5.x Advanced Web Tools administrator guide

Contents

Figures

Tables

About this guide

This guide provides information about:

- Using Advanced Web Tools
- Managing fabrics, switches, and ports
- Routing traffic
- Extended fabrics
- ISL trunking
- Zoning
- Diagnostics
- Fabric Watch

NOTE: FICON is not supported on HP B-Series Fibre Channel switches. The FICON information in this document is included for reference only.

Intended audience

This guide is intended for:

- System administrators responsible for setting up HP StorageWorks Fibre Channel Storage Area Network (SAN) switches
- Technicians responsible for maintaining the Fabric Operating System (OS)

Related documentation

Documentation, including white papers and best practices documents, is available on the HP web site:

http://www.hp.com/country/us/eng/prodserv/storage.html.

IMPORTANT: For late breaking, supplemental information, access the latest version of the *HP StorageWorks Fabric OS 5.x release notes* using the following steps.

To access current Fabric OS related documents:

1. Locate the **IT storage products** section of the web page.
2. Under **Networked storage**, click **SAN infrastructure**.
3. From the **SAN Infrastructure** web page, locate the **SAN Infrastructure products** section.
4. Click **Fibre Channel Switches**.
5. Locate the **B-Series Fabric-Enterprise Class** section. Click **4/256 SAN Director and 4/256 SAN Director power pack**, to access Fabric OS 5.x documents (such as this document).

   The switch overview page displays.
6. Go to the **Product Information section**, located on the right side of the web page.
7. Click **Technical documents.**
8. Follow the onscreen instructions to download the applicable documents.

HP StorageWorks Fabric OS 5.x master glossary

This guide uses industry standard SAN terminology. However, some terms are intrinsic to Fabric OS 5.x. See the *HP StorageWorks Fabric OS 5.x master glossary* for a complete list of terms and definitions.

Access the master glossary from the HP StorageWorks SAN Switch Documentation CD that shipped with your switch. Also, access from the HP web site using the procedure outlined in Related documentation.

Document conventions and symbols

Table 1 Document conventions

Convention	**Element**
Medium blue text: Figure 1	Cross-reference links and e-mail addresses
Medium blue, underlined text (http://www.hp.com)	Web site addresses
Bold font	• Key names • Text typed into a GUI element, such as into a box • GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes
Italics font	Text emphasis
`Monospace font`	• File and directory names • System output • Code • Text typed at the command-line
`Monospace, italic font`	• Code variables • Command line variables
`Monospace, bold font`	Emphasis of file and directory names, system output, code, and text typed at the command line

⚠ **WARNING!** Indicates that failure to follow directions could result in bodily harm or death.

△ **CAUTION:** Indicates that failure to follow directions could result in damage to equipment or data.

IMPORTANT: Provides clarifying information or specific instructions.

NOTE: Provides additional information.

TIP: Provides helpful hints and shortcuts.

HP technical support

Telephone numbers for worldwide technical support are listed on the HP support web site: http://www.hp.com/support/.

Collect the following information before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages

- Operating system type and revision level
- Detailed, specific questions

For continuous quality improvement, calls may be recorded or monitored.

HP strongly recommends that customers sign up online using the Subscriber's choice web site: http://www.hp.com/go/e-updates.

- Subscribing to this service provides you with e-mail updates on the latest product enhancements, newest versions of drivers, and firmware documentation updates as well as instant access to numerous other product resources.
- After signing up, you can quickly locate your products by selecting **Business support** and then **Storage** under Product Category.

HP-authorized reseller

For the name of your nearest HP-authorized reseller:

- In the United States, call 1-800-282-6672.
- Elsewhere, visit the HP web site: http://www.hp.com. Then click **Contact HP** to find locations and telephone numbers.

Helpful web sites

For other product information, see the following HP web sites:

- http://www.hp.com
- http://www.hp.com/go/storage
- http://www.hp.com/support/
- http://www.docs.hp.com

1 Introducing Advanced Web Tools

HP StorageWorks Fabric OS 5.x Advanced Web Tools is a GUI that enables administrators to monitor and manage single or small fabrics, switches, and ports from a standard workstation. It is an optionally licensed product that runs on HP Fabric OS.

Advanced Web Tools provides the administrative control point for HP Advanced Fabric Services, including Advanced Zoning, Interswitch Link (ISL) Trunking, Advanced Performance Monitoring, and Fabric Watch. Advanced Web Tools also provides an interface to telnet commands to perform special switch functions and diagnostics that are available only through the telnet interface.

This chapter contains the following sections:

- What's New in This Document, next
- Requirements, installation, and support, page 15
- Launching Advanced Web Tools, page 20
- Logging in, page 21
- Logging out, page 22
- Session management, page 22

What's New in This Document

The following changes have been made since this document was last released:

- Information that was added:
  - Upfront login and the switchAdmin role are described in "Logging in" on page 21.
  - Support for the 4/256 SAN Director and the 4/16 SAN Switch is added throughout.
- Information that was changed:
  - Changes to the FICON CUP tab are described in "Configuring CUP port connectivity" on page 117.

For further information, see the release notes.

Requirements, installation, and support

Before you install Advanced Web Tools on your workstation, verify that your switches and workstation meet the Advanced Web Tools requirements listed in this chapter.

This section contains the following subsections:

- Requirements, page 15
- Installing an Advanced Web Tools license, page 18
- Value line licenses, page 19
- Switch support, page 19
- Launching Advanced Web Tools, page 20

Requirements

Advanced Web Tools requires a browser that conforms to HTML version 4.0, JavaScript version 1.0, and Java^{TM} Plug-in 1.4.2_06 or later.

HP has certified and tested Advanced Web Tools on the platforms shown in Table 2.

Table 2 Certified and tested platforms

Operating system	Browser	Java Plug-in
Solaris 2.8	Mozilla 1.6	1.4.2_06
Solaris 2.9	Mozilla 1.6	1.4.2_06
Windows® 2000	Internet Explorer 6.0	1.4.2_06
Windows 2003	Internet Explorer 6.0	1.4.2_06
Windows XP®	Internet Explorer 6.0	1.4.2_06

In addition, HP has tested Advanced Web Tools on the platforms shown in Table 3.

Table 3 Tested platforms

Operating system	Browser	Java Plug-in
Red Hat Linux® 9.0	Mozilla 1.6	1.4.2_06

NOTE: Some browsers must be configured to work with Advanced Web Tools. For information about how to do this, see the section "Configuring Internet Explorer," next.

Adequate RAM is required on Windows systems:

- 256 MB or more RAM for fabrics comprising 15 switches or less
- 512 MB or more RAM for fabrics comprising more than 15 switches

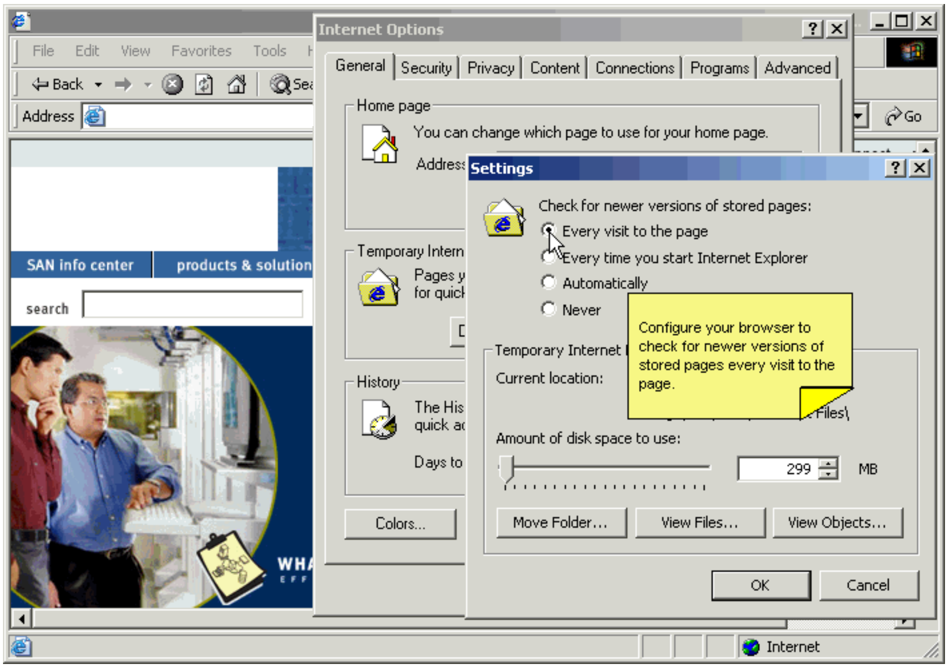
HP recommends a minimum of 8 MB of video RAM.

Configuring Internet Explorer

Correct operation of Advanced Web Tools with Internet Explorer requires specifying the appropriate settings for browser refresh frequency and process model. Browser pages should be refreshed frequently to ensure the correct operation of Advanced Web Tools.

Setting the refresh frequency

1. Select **Tools > Internet Options** in the browser.
2. Select the **General** tab and click **Settings** (under Temporary Internet Files).
3. Click **Every visit to the page** under Check for newer versions of stored pages, as shown in Figure 1.



File Edit View Favorites Tools
Back
Address
SAN info center
products & solution
search
Internet Options
General Security Privacy Content Connections Programs Advanced
Home page
You can change which page to use for your home page.
Temporary Intern
History
Colors...
Go
Internet

Settings

Check for newer versions of stored pages:

- ● Every visit to the page
- ○ Every time you start Internet Explorer
- ○ Automatically
- ○ Never

Configure your browser to check for newer versions of stored pages every visit to the page.

Temporary Internet
Current location:

Amount of disk space to use: 299 MB

Figure 1 Configuring Internet Explorer

Installing Java on the workstation

Java Plug-in version 1.4.2_06 must be installed on the workstation for the correct operation of Advanced Web Tools.

If you try to launch Advanced Web Tools without any Java Plug-in installed:

- Internet Explorer prompts and downloads the proper Java Plug-in.
- Mozilla downloads the most recently released Java Plug-in.

If you try to launch Advanced Web Tools with an earlier version Java Plug-in installed,

- Internet Explorer might prompt you for an upgrade, depending on the existing Java Plug-in version.
- Mozilla uses the existing Java Plug-in.

Installing the JRE on your Solaris or Linux client workstation

1. Locate the Java Runtime Environment (JRE) on the Internet, at the following URL:
   http://java.sun.com/products/archive/j2se/1.4.2_06/index.html

NOTE: This URL points to a non-HP web site and is subject to change without notice.

2. Follow the instructions to install the JRE.
3. Create a symbolic link from `$MOZILLA/plugins/libjavaplugin_oji.so` to `$JRE/plugin/$ARCH/ns600/libjavaplugin_oji.so`

Installing patches on Solaris

1. Search for any required patches for your current version of the JRE at the following web site:
   http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage

NOTE: This URL points to a non-HP web site and is subject to change without notice.

2. Follow the link to download the patch, and exit the browser when you are done.
3. Install the patch and reboot the system.

Installing the Java Plug-in on Windows

1. Select **Start Menu > Settings > Control Panel** and then select the **Java Plug-in Control Panel**.
2. Select the **About** tab.
3. Determine whether the correct Java Plug-in version is installed:
   - If the correct version is installed, Advanced Web Tools is ready to use.
   - If no Java Plug-in is installed, point the browser toward a switch running Fabric OS 4.x or later, follow the link to the Sun Microsystems web site, download the correct Java Plug-in, and double-click the downloaded file to install the plug-in.
   - If an outdated version is currently installed, uninstall it, relaunch the browser, and enter the address of a switch running Fabric OS 4.4.0 or later. Advanced Web Tools guides you through the steps to download the proper Java Plug-in.

Installing an Advanced Web Tools license

You can install an Advanced Web Tools license either through telnet or over the Web.

All licenses, including Advanced Web Tools licenses, are installed on a chassis basis. For example, if you install an Advanced Web Tools license on logical switch 0 in a Core Switch 2/64, you do not need to install an additional Advanced Web Tools license on logical switch 1 of that Core Switch 2/64, because both are in the same chassis.

To determine whether a license is already installed on a switch, follow the instructions provided in the section "Installing an Advanced Web Tools license through telnet," next. If a license is not installed, contact your switch supplier to obtain a license key.

Installing an Advanced Web Tools license through telnet

Use the following procedure to determine whether an Advanced Web Tools license is installed on your switch and, if not, install it.

Installing an Advanced Web Tools license through telnet

1. Log in to the switch via telnet (see the *HP StorageWorks Fabric OS 5.x administrator guide* for more information), using an account that has administrative privileges.
2. To determine whether an Advanced Web Tools license is already installed on the switch, enter `licenseShow` on the telnet command line.

   A list is displayed, showing all the licenses currently installed on the switch:

   ```
   switch:admin> licenseshow
   1A1AaAaaaAAAA1a: ]-- This is the license key. The installed feature is
   listed below.
       Zoning license
   1A3AaAbcbBBCC1d:
       QuickLoop license
   ```

   If the Advanced Web Tools license is not included in the list or is incorrect, continue with step 3.
3. On the command line, enter:

   ```
   licenseadd key
   ```

   where *`key`* is the license key. The license key value is case-sensitive and must be entered exactly as given.
4. Verify that the license was added by typing the following command:

   ```
   licenseshow
   ```

   If the Advanced Web Tools license is listed, the feature is available. If the license is not listed, repeat step 3.

Installing an Advanced Web Tools license through the web

Launching Advanced Web Tools from any nonlicensed switch opens the license dialog box. If the fabric already contains at least one licensed switch, you can use Advanced Web Tools to view and license other switches from the licensed switch.

Installing the first license through the web

1. Launch the web browser and enter the IP address of the switch in the Location/Address field:

   ```
   http://10.77.77.77
   ```

2. Press **Enter**.

   If an Advanced Web Tools license is already installed on the switch, Advanced Web Tools launches. If no license is installed, a license dialog box opens.

3. If the license dialog box opens, follow the instructions provided.

Installing additional licenses through the web

1. Launch the Web browser and enter the IP address of the licensed switch in the **Location/Address** field:

   ```
   http://10.77.77.77
   ```

2. Press **Enter**.

   Advanced Web Tools opens, displaying the Switch Explorer.

3. Click the icon for the switch to which you want to add a license.

   A licensing window opens.

4. Follow the instructions provided.

Value line licenses

If your fabric includes a switch with a limited switch license and you are launching Advanced Web Tools using that switch, and if the fabric exceeds the switch limit indicated in the license, Advanced Web Tools allows a 45-day grace period in which you can still monitor the switch through Advanced Web Tools. However, Advanced Web Tools displays warning messages periodically.

These messages warn you that your fabric size exceeds the supported switch configuration limit and tells you how long you have before Advanced Web Tools will be disabled. After the 45-day grace period, you will no longer be able to launch Advanced Web Tools from the switch with the limited switch license if that switch is still exceeding the switch limit.

Value line fabric licensing is applicable only to the SAN Switch 2/8V and SAN Switch 2/16V. These licenses are indicated by `2 Domain Fabric` and `4 Domain Fabric` in the License tab of the Switch Admin module. See "Maintaining licensed features" on page 47 for more information.

Switch support

You can use Advanced Web Tools 5.x with the following HP StorageWorks switches and directors:

- 4/8 SAN Switch
- SAN Switch 2/16
- SAN Switch 2/8V
- SAN Switch 2/16V
- SAN Switch 2/32
- 4/16 SAN Switch
- SAN Switch 4/32
- Core Switch 2/64
- SAN Director 2/128
- 4/256 SAN Director
- Brocade 4Gb SAN Switch for HP p-Class BladeSystem

Advanced Web Tools is part of the Fabric OS of a switch. When you launch Advanced Web Tools on a switch, you can manage other switches in the fabric that have lower or higher firmware versions. It is important to note that when accessing these switches you are opening the remote switch's version of Advanced Web Tools, and the functionality available for those switches might vary.

Launching Advanced Web Tools

You can launch Advanced Web Tools on any workstation with a compatible web browser installed. For a list of web browsers compatible with Fabric OS 5.x, see Table 2 on page 16 and Table 3 on page 16. Advanced Web Tools also supports HTTPS protocol, if that protocol is enabled for the switch. For more information on enabling the HTTPS protocol on your switch, see the *HP StorageWorks Fabric OS 5.x administrator guide*.

Launching Advanced Web Tools

1. Launch the web browser and enter the IP address of the licensed switch in the Address field:

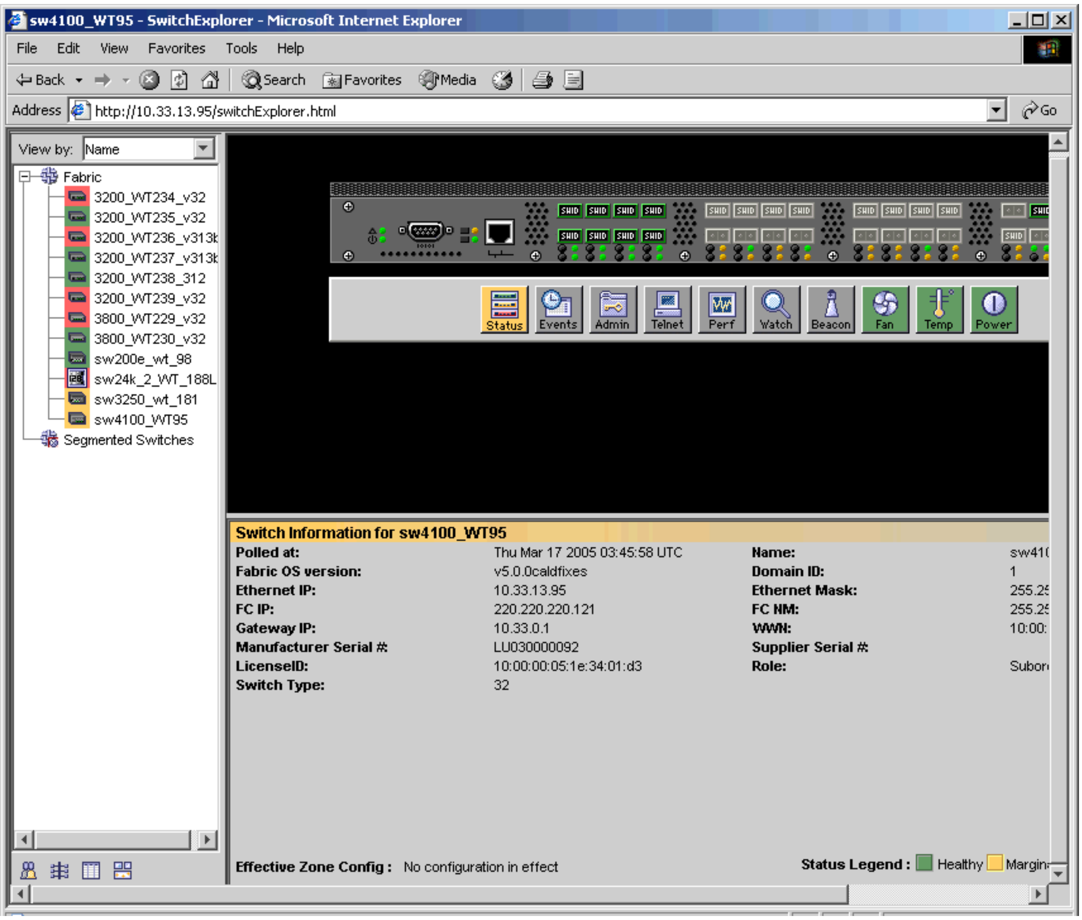
   `http://10.77.77.77` or `https://10.77.77.77`

2. Press **Enter**.

   Depending on the switch is configuration, you might be prompted to log in to the switch at this time. See "Advanced Web Tools interface" on page 20 for more information.

Advanced Web Tools

Advanced Web Tools launches, as shown in Figure 2. Go to Chapter 3, Using Advanced Web Tools for instructions on using this interface.



Address: http://10.33.13.95/switchExplorer.html

Switch Information for sw4100_WT95

Polled at:	Thu Mar 17 2005 03:45:58 UTC	**Name:**	sw41
Fabric OS version:	v5.0.0caldfixes	**Domain ID:**	1
Ethernet IP:	10.33.13.95	**Ethernet Mask:**	255.25
FC IP:	220.220.220.121	**FC NM:**	255.25
Gateway IP:	10.33.0.1	**WWN:**	10:00:
Manufacturer Serial #:	LU030000092	**Supplier Serial #:**	
LicenseID:	10:00:00:05:1e:34:01:d3	**Role:**	Subor
Switch Type:	32		

Effective Zone Config : No configuration in effect

Figure 2 Advanced Web Tools interface

Logging in

When you use Advanced Web Tools, you must log in before you can modify any switch information. This section describes upfront login, which determines when you log in, and role-based access control, which is determined by how you log in.

Prior to displaying the login window, Advanced Web Tools displays a security banner (if one is configured for your switch), which you must accept before logging in. The security banner is displayed every time you log in, regardless of whether upfront login is enabled.

Upfront login

Depending on how your switch is configured, you are either prompted to log in once, when you launch Advanced Web Tools (upfront login), or you are prompted to log in whenever you launch a switch administration module, such as the Switch Admin or Zoning module.

By default, upfront login is disabled. Use the `configure` telnet command to enable or disable upfront login. See the *HP StorageWorks Fabric OS 5.x command reference guide* for information.

Table 4 lists different behaviors, depending on whether upfront login is enabled.

Table 4 Comparison of login modes

Upfront login enabled	**Upfront login not enabled**
You must log in before you see the Switch Explorer (shown in Figure 2 on page 20).	Switch Explorer launches with no login.
A single session is shared by the Switch Explorer and all child windows launched from it. (See "Session management" on page 22 for more information on sessions.)	Switch Admin, Zone Admin, and other protected modules require separate login. (These modules are described in subsequent chapters.)
Role-based access control is enforced across the entire session. (See Role-based access control next, for more information.)	Role-based access control is enforced on a per-module basis.
When you log out or close Switch Explorer, all windows belonging to the session are invalided. (See "Logging out" on page 22 for more information.)	There is no Logout button in Switch Explorer. Closing the Switch Explorer window does not invalidate other windows that were opened from it.
If you refresh the Switch Explorer window, all windows belonging to the session are invalidated.	Refreshing the Switch Explorer window does not affect other windows that were opened from it.
Inactivity timeout (two hours) invalidates the Switch Explorer and all windows opened from it.	Inactivity timeout applies only to protected modules, and each module has its own session. This means that if the Switch Admin module times out, the Zone Admin module could still be left open. Conversely, recent activity in the Switch Admin module does not prevent the Zone Admin module from timing out if there is no activity in that module.

Role-based access control

You can log in at the admin, switchAdmin, or user level. Each role gives you a different access level:

admin — You have full access to all of the Advanced Web Tools functionality.

switchAdmin — You can do everything the admin role can do, except for the following:

- You cannot modify zoning configurations.
- You cannot create new accounts.

You cannot view or change account information for any accounts. You can view only your own account and change your account password.

user — You can view switch information but cannot access any of the switch administration modules.

When upfront login is enabled and the security banner is set on a switch, users are required to log in at user level or higher to launch individual modules.

When upfront login is disabled and the security banner is set on a switch, users are required to log in at admin level to launch individual modules.

Logging in

1. Click **OK** in the security banner window, if one appears.

   The login window opens.
2. Enter the user name of an account with the admin, switchAdmin, or user role.
3. Enter the password.
4. Click **OK**.

Logging out

If upfront login is enabled, you can end your Advanced Web Tools session either by logging out or by closing the Switch Explorer browser window. All windows belonging to the session are invalidated (after a short delay they become grayed out and unusable, but you must close them manually).

If upfront login is not enabled, each module that you have logged in to is a separate session. You need to close each module to end each session. Closing the Switch Explorer does not invalidate these other sessions.

Ending an Advanced Web Tools session with upfront login enabled

Click **Logout** in the Switch Explorer or click the X in the upper right corner of the Switch Explorer browser window to close it.

Session management

A *Web Tools session* is defined as the connection between the Advanced Web Tools client and its managed switch.

A session is established when you log in to a switch through Advanced Web Tools. The scope of the session depends on whether upfront login is enabled:

- If upfront login is enabled, a single session is shared by the Switch Explorer and all child windows launched from it. Closing or navigating away from the Switch Explorer ends the session and invalidates all related child windows. Closing the child windows, however, does not end the session.
- If upfront login is not enabled, a session encompasses only the child window to which you are logged in (such as the Switch Admin, Zone Admin, and other protected modules). You can open multiple sessions from the same Switch Explorer window. Closing or navigating away from the Switch Explorer does not close the session or affect the child windows.

A session remains in effect until one of the following happens:

- You log out.
- You close or navigate away from the Switch Explorer window (if upfront login is enabled).
- You refresh the Switch Explorer window (if upfront login is enabled).
- You close the child window (if upfront login is disabled).
- The session times out due to inactivity.

A session times out if it has been inactive for longer than two hours. Inactivity does not mean that there is no user activity (such as keystrokes or mouse movements); it means that no information is sent to the switch (by clicking Apply or Save buttons). For example, in the Zoning module you can spend a lot of time setting up a zoning scheme without actually sending information to the switch. Advanced Web Tools does not display a warning when the session is about to time out. If the session times out, you must restart Advanced Web Tools and log in again.

Advanced Web Tools enables sessions to both secure and nonsecure switches.

2 Using Advanced Web Tools

This chapter contains the following sections:

Viewing the Switch Explorer

The first thing you see when you log in to a switch with Advanced Web Tools is the Switch Explorer (see Figure 3). The Switch Explorer is divided into several areas that provide access to and information about the switch and fabric. You should familiarize yourself with these areas, as the procedures in this guide refer to them as follows:

- Fabric Tree, which displays a list of all the switches in the fabric
- Fabric Toolbar, which provides access to fabric-wide management interfaces, such as Name Server, zoning, and events
- Switch View, which displays an interactive graphical representation of the switch
- Switch View Button Menu, which displays buttons providing switch information such as status, event information, access to telnet, switch administration, switch performance, beaconing, and much more
- Switch Information View, which displays information about the switch such as name, status, Fabric OS version, domain ID, IP address, and WWN
- Status Legend, which defines the meaning of the colors visible in the background of various icons in the Switch Explorer

These areas are described further in the sections that follow.

Clicking some of the buttons and icons in the Switch Explorer opens up a separate module, from which you can perform management tasks. In this document, a *module* is a collection of related tabs or views that are displayed in a single browser window. The zoning module and the Switch Admin module require you to log in, if upfront login is not enabled.

The format of the Switch Explorer varies, depending on the hardware type. Figure 3 through Figure 6 on page 29 show Switch Explorer examples for several HP StorageWorks switches.

Note that the figures are grayed out so that you can more easily see the areas of the Switch Explorer.

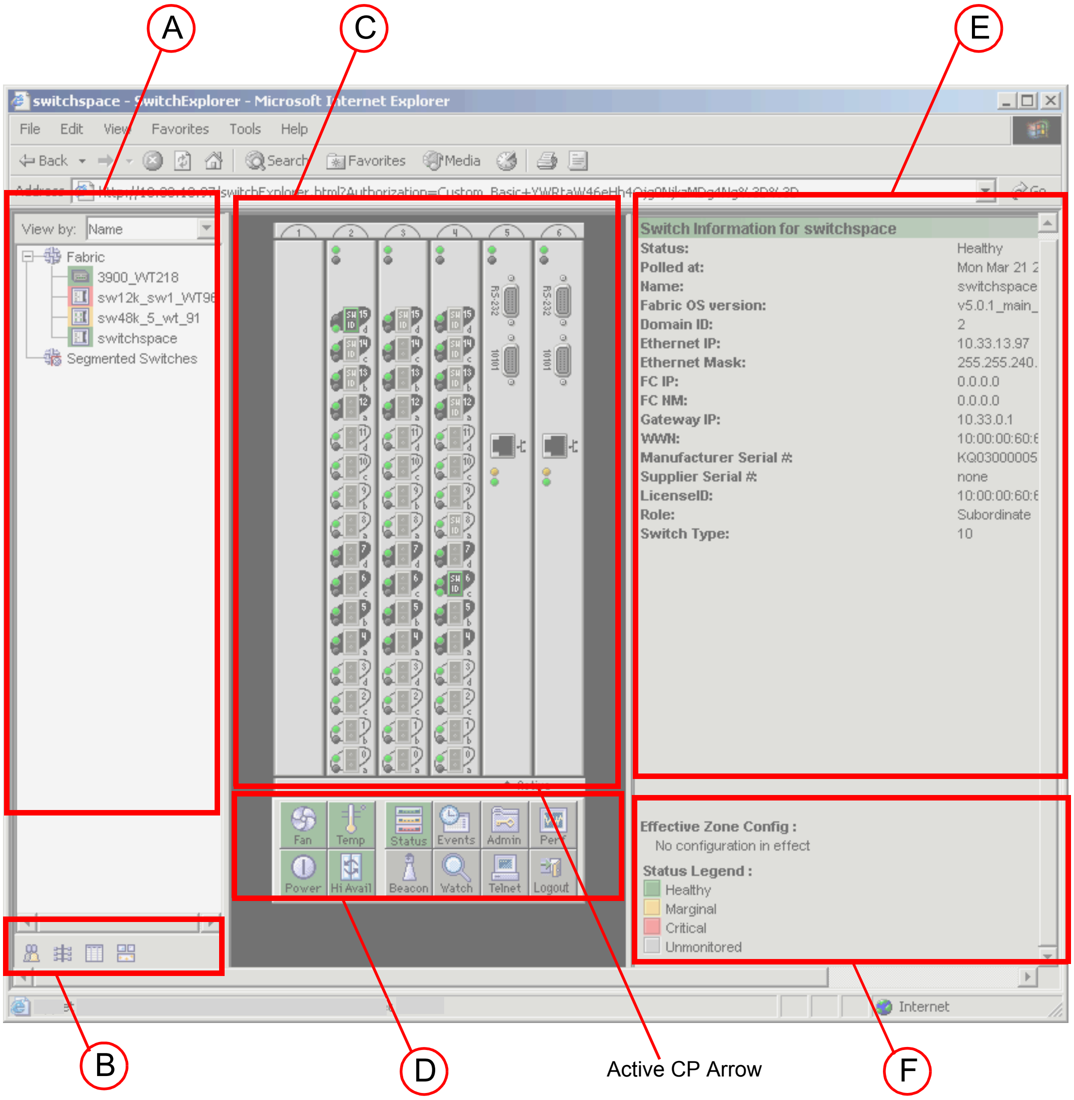
In Figure 3 through Figure 6 on page 29, the letters A through F call out the different areas within the Switch Explorer. Table 5 is a key for these callouts.

Table 5 Key to Figure 3 through Figure 6

Callout	Area of Switch Explorer view
A	Fabric tree
B	Fabric toolbar
C	Switch view
D	Switch view button menu
E	Switch information view
F	Status legend

Core Switch 2/64

Figure 3 shows an example of the Advanced Web Tools Switch Explorer for a Core Switch 2/64.



Switch Information for switchspace

Status:	Healthy
Polled at:	Mon Mar 21 2
Name:	switchspace
Fabric OS version:	v5.0.1_main_
Domain ID:	2
Ethernet IP:	10.33.13.97
Ethernet Mask:	255.255.240.
FC IP:	0.0.0.0
FC NM:	0.0.0.0
Gateway IP:	10.33.0.1
WWN:	10:00:00:60:6
Manufacturer Serial #:	KQ03000005
Supplier Serial #:	none
LicenseID:	10:00:00:60:6
Role:	Subordinate
Switch Type:	10

Effective Zone Config :
No configuration in effect

Status Legend :
🟩 Healthy
🟨 Marginal
🟥 Critical
⬜ Unmonitored

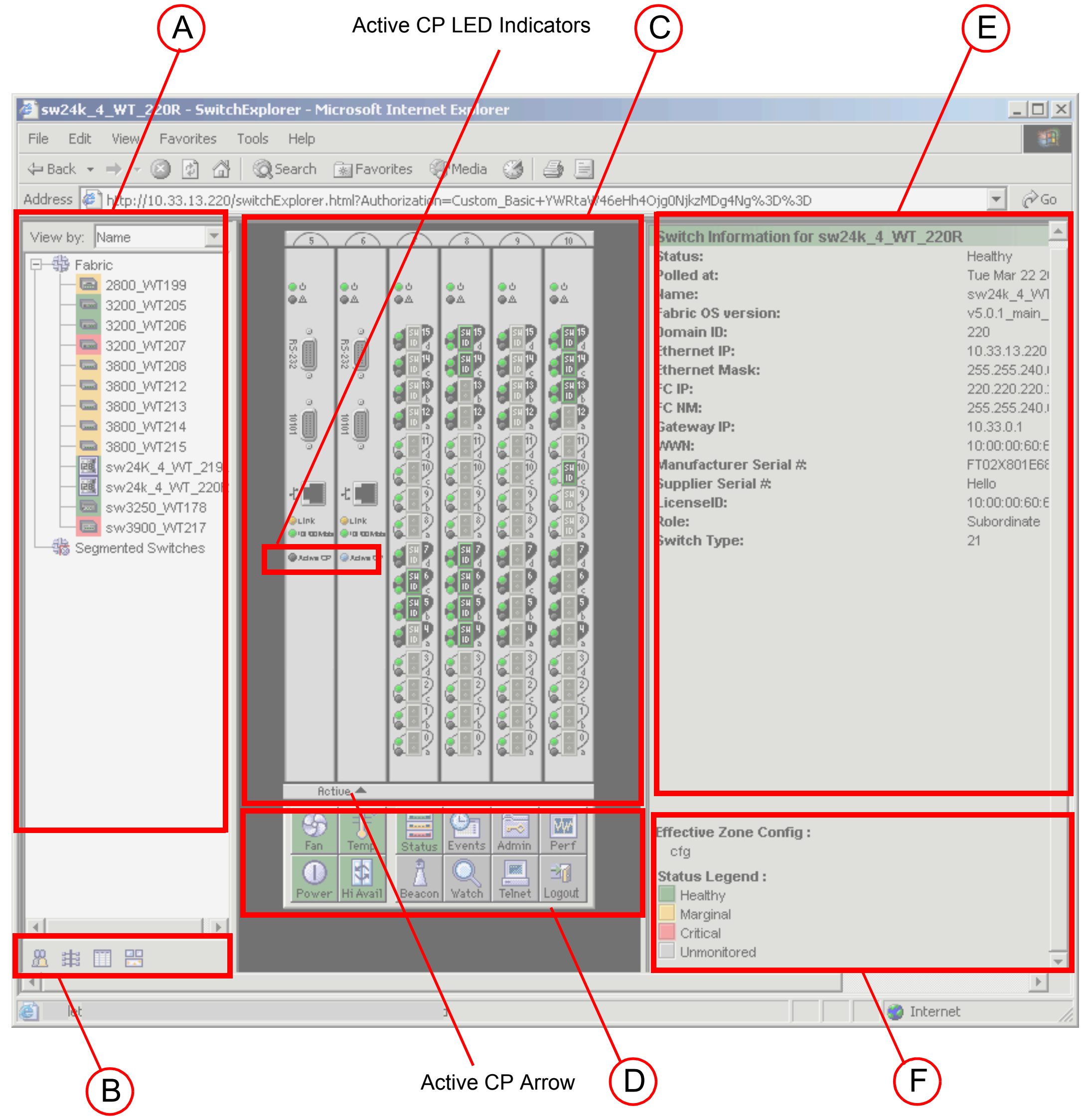
Figure 3 Advanced Web Tools Switch Explorer for a Core Switch 2/64

In this figure, the Core Switch 2/64 has two domains; however, only one domain is displayed. You can view and manage only one domain at a time, even though both domains are enclosed in the same chassis. To manage the other domain, you must log in to it separately.

The active control processor (CP) in the Core Switch 2/64 is labeled with a small arrow at the bottom of the CP.

SAN Director 2/128

Figure 4 shows an example of the Advanced Web Tools Switch Explorer for a SAN Director 2/128 (see the legend in Table 5 on page 25). In this figure, the SAN Director 2/128 has two domains; only one domain is displayed. You can view and manage only one domain at a time, even though both domains are enclosed in the same chassis. To manage the other domain, you must log in to it separately.



Switch Information for sw24k_4_WT_220R

Status:	Healthy
Polled at:	Tue Mar 22 2
Name:	sw24k_4_WT
Fabric OS version:	v5.0.1_main_
Domain ID:	220
Ethernet IP:	10.33.13.220
Ethernet Mask:	255.255.240.
FC IP:	220.220.220.
FC NM:	255.255.240.
Gateway IP:	10.33.0.1
WWN:	10:00:00:60:6
Manufacturer Serial #:	FT02X801E6
Supplier Serial #:	Hello
LicenseID:	10:00:00:60:6
Role:	Subordinate
Switch Type:	21

Effective Zone Config :
cfg

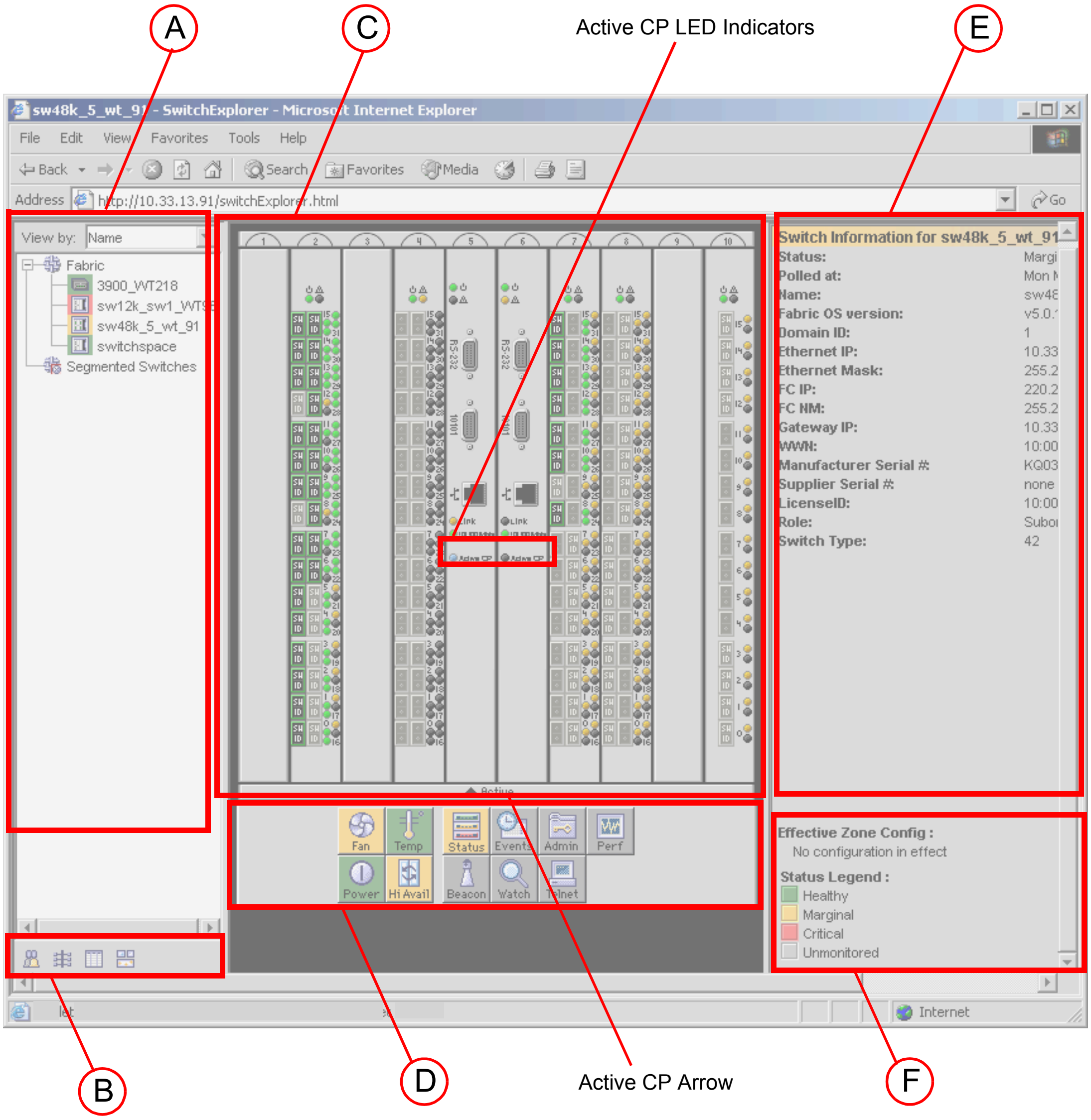
Status Legend :
🟩 Healthy
🟨 Marginal
🟥 Critical
□ Unmonitored

Figure 4 Advanced Web Tools Switch Explorer for a SAN Director 2/128

The active CP in the SAN Director 2/128 is labeled with a small arrow at the bottom of the CP display. The SAN Director 2/128 active CP is also indicated with the blue Active CP LED indicator, as shown in the figure.

4/256 SAN Director

Although the 4/256 SAN Director has a single chassis, it can contain one domain or two domains. Figure 5 shows an example of the Advanced Web Tools Switch Explorer for a single-domain 4/256 SAN Director (see the legend in Table 5 on page 25).



Switch Information for sw48k_5_wt_91

Status:	Margi
Polled at:	Mon M
Name:	sw48
Fabric OS version:	v5.0.1
Domain ID:	1
Ethernet IP:	10.33
Ethernet Mask:	255.2
FC IP:	220.2
FC NM:	255.2
Gateway IP:	10.33
WWN:	10:00
Manufacturer Serial #:	KQ03
Supplier Serial #:	none
LicenseID:	10:00
Role:	Subor
Switch Type:	42

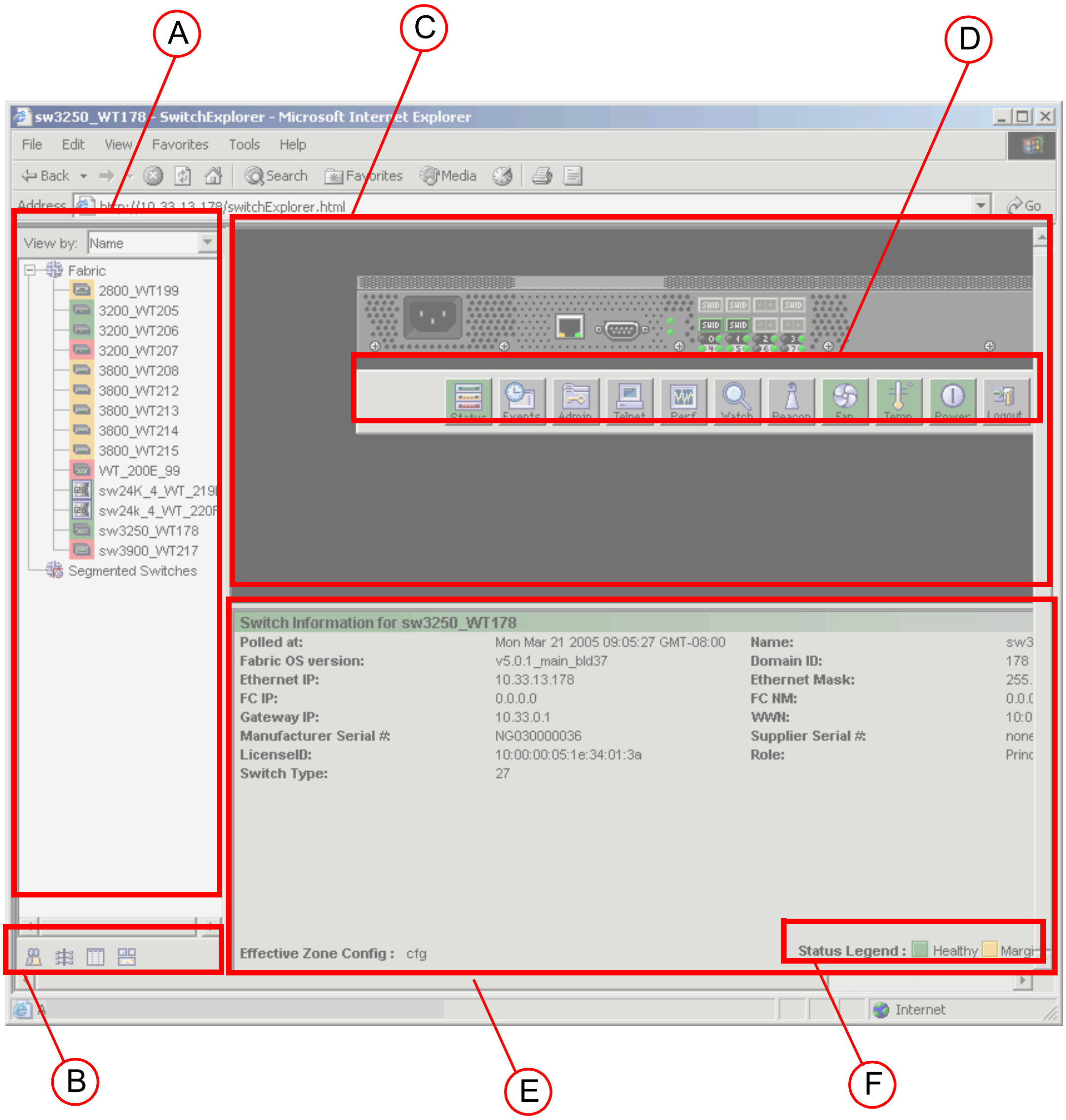
Effective Zone Config :
No configuration in effect

Status Legend :
🟩 Healthy
🟨 Marginal
🟥 Critical
□ Unmonitored

Figure 5 Advanced Web Tools Switch Explorer for a 4/256 SAN Director

SAN Switch 2/8V

Figure 6 shows an example of the Advanced Web Tools Switch Explorer for a SAN Switch 2/8V (see the legend in Table 5 on page 25). This is the same format as the Switch Explorer used in Advanced Web Tools for the 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/16V, SAN Switch 2/32, and SAN Switch 4/32.



Switch Information for sw3250_WT178

Polled at:	Mon Mar 21 2005 09:05:27 GMT-08:00	Name:	sw3
Fabric OS version:	v5.0.1_main_bld37	Domain ID:	178
Ethernet IP:	10.33.13.178	Ethernet Mask:	255.
FC IP:	0.0.0.0	FC NM:	0.0.0
Gateway IP:	10.33.0.1	WWN:	10:0
Manufacturer Serial #:	NG030000036	Supplier Serial #:	none
LicenseID:	10:00:00:05:1e:34:01:3a	Role:	Princ
Switch Type:	27		

Effective Zone Config : cfg

Status Legend : 🟩 Healthy 🟨 Margi

Figure 6 Advanced Web Tools Switch Explorer for a SAN Switch 2/8V

Refresh rates

Different panels of Advanced Web Tools refresh at different rates. Table 6 lists the polling rates for the various panels in Advanced Web Tools.

Table 6 Polling rate in the Switch Explorer window

Switch explorer area	Polling rate
Name Server	User-defined; 15 seconds minimum
Zoning Database	60 seconds
Fabric Watch	15 seconds
Performance Monitor	30 seconds

The refresh, or polling, rates listed in this section and throughout the book indicate the time between the end of one polling and the start of the next, and *not* how often the screen is refreshed. That is, a refresh rate of 15 seconds does not mean that a refresh occurs every 15 seconds. It means that a new refresh starts 15 seconds after the previous refresh finished.

Fabric Tree

The Fabric Tree is the left panel of the Switch Explorer. The Fabric Tree displays all switches in the fabric, including switches that do not have an Advanced Web Tools license. Any switches segmented before Advanced Web Tools is launched are not displayed.

Although all switches in the fabric are displayed, only switches that have an Advanced Web Tools license installed can be managed through Advanced Web Tools. Other switches must be managed through the Fabric OS command line interface (CLI) or another management application. For information on adding an Advanced Web Tools license to a switch, see "Installing an Advanced Web Tools license" on page 18.

Use the drop-down menu at the top of the panel to view switches in the Fabric Tree by switch name, IP address, or WWN. The background color of the switch icon indicates the current status of the switch. You can mouse-over a switch in the fabric tree to display the IP address and current status.

You can manually refresh the status of a switch within the fabric by right-clicking that switch in the Fabric Tree and clicking **Refresh**.

Fabric toolbar

The Fabric Toolbar at the bottom of the Fabric Tree enables you to access fabric-wide administration tasks quickly. The Fabric Toolbar icons provide access to:

- Fabric events

  This information is collected from the launch switch. See "Monitoring events" on page 50 for more information.
- Topology module

  This information is collected from the selected switch. See "Displaying a fabric topology report" on page 55 for more information.
- Name Server information

  This information is collected from the selected switch. See "Displaying the Name Server entries" on page 55 for more information.
- Zone Administration module

  This information is collected from the selected switch. This icon is displayed only if an HP Advanced Zoning license is installed on the switch. If secure mode is enabled, zoning can be administered only from the primary fabric configuration server (FCS) switch. If the selected switch has a zoning license installed but is not the primary switch, the Zone Admin icon is displayed but not activated. See "Managing zoning with Advanced Web Tools" on page 81 for more information.

It is important to note that the information displayed is gathered from different areas; switches in the fabric might be running different versions of Fabric OS, and different versions of Fabric OS support different features, so the information displayed might not always be the same for switches running different versions of Fabric OS.

Switch View

The Switch View displays a graphical representation of the selected switch, including a real-time view of switch and port status. This view is accessed by selecting a switch icon in the Fabric Tree.

NOTE: The Switch View display is updated approximately once every 15 seconds. However, the initial display of the Switch Explorer might take from 30 to 60 seconds after the switch is booted.

The layout of information is different for the Switch View of different switch types. See Figure 3 on page 26 through Figure 6 on page 29 for examples of different Switch Views.

Switch View button menu

The Switch View button menu is the launch point for the Switch Events screen, telnet interface, Fabric Watch module, Switch Admin module, Performance Monitor module, and High Availability (HA) Admin module. Some of these functions require a license key to activate. The Switch View button menu also includes buttons that display the status of the switch fans, temperature monitors, switch information, power supply, and beacon. If upfront login is enabled, the Switch View button menu also includes a Logout button.

It is important to note that certain Fabric OS features are available only on particular switch types; therefore, the icons for those features are displayed only for those switch types. For example, the HA feature is available only on the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director; therefore, the HA Admin button is displayed in the Switch View button menu only for those directors.

The following buttons have a color-coded background, which indicates status for that area:

- Status
- Fan
- Temp
- Power
- Hi Avail (HA)

The colors follow the status legend (see "Status Legend").

Switch Information View

The Switch Information View displays vital switch information such as name, status, Fabric OS version, domain ID, IP address, WWN, and current zone configuration. The information in the Switch Information View is polled every 15 seconds.

The Switch Information View is located beside the graphic representation of the switch for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director. For all other switch types (4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, 4Gb SAN Switch for HP p-Class BladeSystem, and SAN Switch 4/32), the Switch Information View is located beneath the graphic representation of the switch.

For more information, see "Displaying switch information" on page 105.

Status Legend

The Status Legend is included in the Switch Information View and defines the meaning of colors visible in the background of the various icons in the Switch Explorer. Each color indicates a different operational state:

- Green: healthy
- Yellow: marginal
- Red: critical
- Gray: unknown or unmonitored

NOTE: For all status displays based on errors per time interval, any errors cause the status to show faulty until the entire sample interval has passed.

Displaying switches in the fabric

If your fabric has more than one switch, you can launch Advanced Web Tools from one switch and then access other switches.

Accessing the Switch Explorer for a particular switch

1. Launch Advanced Web Tools as described in "Launching Advanced Web Tools" on page 20.

   The Switch Explorer is displayed for the switch you logged in to. The Fabric Tree is expanded by default when you first launch Advanced Web Tools.
2. If the Fabric Tree is not expanded, click the **+** in the Fabric Tree to view all the switches in the fabric.
3. Click a switch in the Fabric Tree.

   A separate browser window opens and displays the selected switch. (If the launch switch is running a Fabric OS version earlier than 5.0.1, the selected switch is displayed in the same browser window.)

   The graphic of the selected switch is displayed in the "Switch View" on page 31. Additional switch information is displayed in the "Switch Information View" on page 31.

Ending the Advanced Web Tools session

You can end your Advanced Web Tools session either by logging out or by closing the Switch Explorer browser window.

A session times out if it has been inactive for longer than two hours. If the session times out, you must restart Advanced Web Tools and log in again. See "Session management" on page 22 for more information about sessions.

Ending the Advanced Web Tools session

Click **Logout** in the Switch Explorer (the logout button is displayed only if upfront login is enabled) or click the **X** in the upper-right corner of the Switch Explorer browser window to close the window.

Using Advanced Web Tools and secure mode

When secure mode is enabled on switches you manage through Advanced Web Tools, there are certain requirements and scenarios you should be aware of. You should read through the requirements and scenarios in this section if you plan to use Advanced Web Tools to manage any switches that have secure mode enabled.

Advanced Web Tools access and HTTP_POLICY

When secure mode is enabled, access to the Advanced Web Tools interface is controlled by HTTP_POLICY. If secure mode is enabled and HTTP_POLICY has been defined, your workstation IP address must be included in this policy or you will not have access to Advanced Web Tools for any switch in the fabric. If your workstation IP address is not included in this policy, the Interface Disabled page is displayed when you attempt to access a switch. For instructions on including your workstation in HTTP_POLICY, see the *HP StorageWorks Secure Fabric OS administrator guide*.

NOTE: If a secure mode change is made in the fabric—that is, secure mode is enabled, secure mode is disabled, or there is a change to the primary FCS—you must exit and relaunch Advanced Web Tools. If Advanced Web Tools is kept open after a secure mode change occurs, behavior is undefined.

Opening modules in a secure fabric

When opening more than one module in a secure fabric, wait for each module to load completely before opening another. For example, if you want to access both the Zone Admin and the Switch Admin modules, open one of the modules and wait for it to load completely before opening the second module. Abnormal behavior might occur if you attempt to open two modules simultaneously in a fabric with secure mode enabled.

Certain Advanced Web Tools features are limited or disabled when secure mode is enabled on a fabric. For more information about secure mode, see the *HP StorageWorks Secure Fabric OS administrator guide*.

Primary-FCS-only functionality

The following Advanced Web Tools functionality is reserved for the primary FCS when secure mode is enabled:

- Zoning administration is allowed only from the primary FCS switch when secure mode is enabled. For all other switches in a secure fabric, the Zoning button is disabled.
- SNMP community strings can be modified only from the primary FCS switch when secure mode is enabled. For non-FCS switches, you can view the SNMP community strings, but they are read-only, and the SNMP access control lists on the SNMP tab are not displayed.
- User account administration is allowed only from the primary FCS switch when secure mode is enabled. The changes are then propagated to all switches in the fabric.

Disabled functionality

Telnet access to a switch and the Telnet button in Advanced Web Tools are both disabled when secure mode is enabled for a fabric. You must use sectelnet or SSH to access the Fabric OS CLI in a secure fabric. These capabilities are not accessible from Advanced Web Tools. For more information on sectelnet or SSH, see the *HP StorageWorks Secure Fabric OS administrator guide*.

The SNMP Access Control List is replaced with RSNMP_POLICY and WSNMP_POLICY when secure mode is enabled for a fabric. The SNMP Access Control List is not displayed in Advanced Web Tools.

Recommendations for working with Advanced Web Tools

Listed below are recommendations when working with Advanced Web Tools:

- When using a mixed fabric—that is a fabric containing switches and directors running 4.x, 3.x, and 2.x firmware—use the most advanced switches or directors to control the fabric. For example, use the 5.x and 4.x switches or directors as the primary FCS, the location to perform zoning tasks, and the time server (CLI). You should use the most recently released firmware on your switches.
- If switches are accessed simultaneously from different connections (for example, Advanced Web Tools, CLI, and API), changes from one connection might not be updated to the other, and some modifications might be lost. Make sure when connecting with simultaneous multiple connections that you do not overwrite the work of another connection.
- Several tasks in Advanced Web Tools make fabric-level changes, for example, the tasks in the Zone Admin module. When executing fabric-level configuration tasks, wait until you have received confirmation that the changes are implemented before executing any subsequent tasks. For a large fabric, this can be up to a few minutes.
- HP recommends a maximum of five simultaneous HTTP sessions to any one switch. An HTTP session is considered a Fabric Manager or Advanced Web Tools connection to the switch.

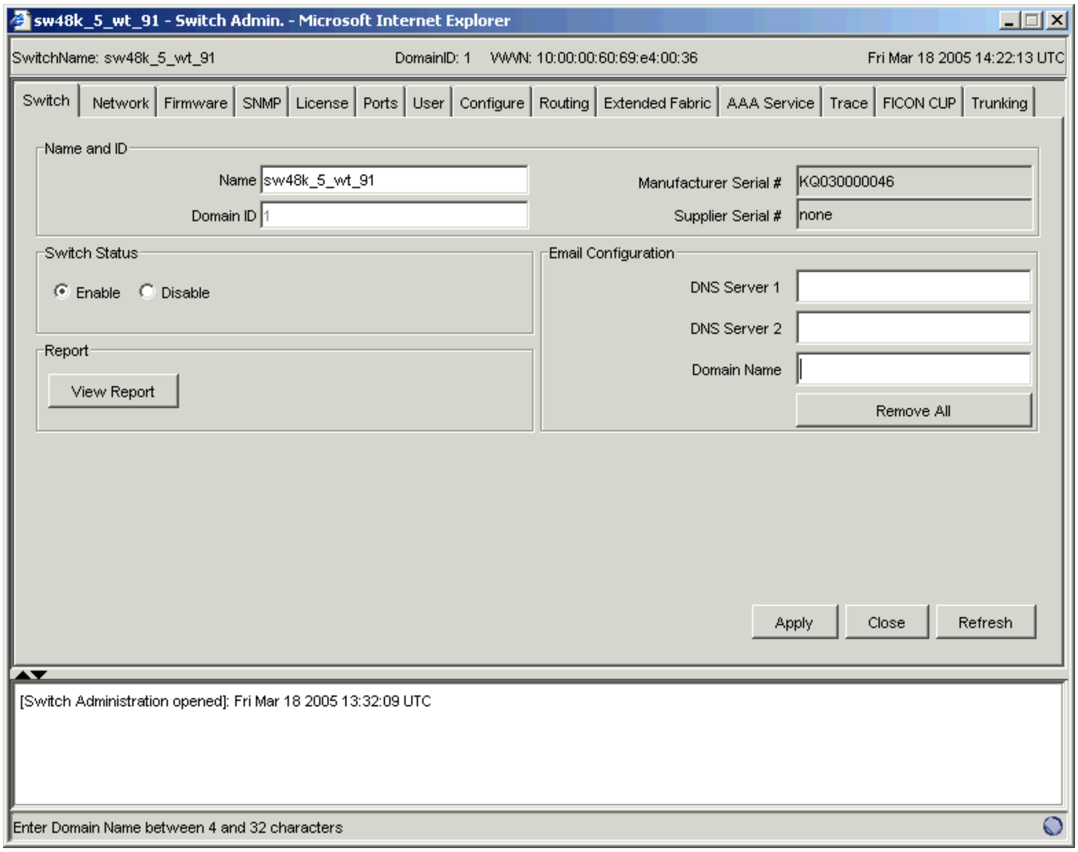
3 Managing your fabrics, switches, and ports

This chapter contains the following sections:

Managing fabrics, switches, and ports using Advanced Web Tools

You can perform most of the management tasks described in this chapter through the Switch Admin module. Information in the Switch Admin module is retrieved from the selected switch.

Click the **Admin** button in the Switch View to access the Switch Admin module. Figure 7 shows the Switch Admin module.



sw48k_5_wt_91 - Switch Admin. - Microsoft Internet Explorer

SwitchName: sw48k_5_wt_91 DomainID: 1 WWN: 10:00:00:60:69:e4:00:36 Fri Mar 18 2005 14:22:13 UTC

Name sw48k_5_wt_91

Domain ID 1

Manufacturer Serial # KQ030000046

Supplier Serial # none

● Enable ○ Disable

[Switch Administration opened]: Fri Mar 18 2005 13:32:09 UTC

Enter Domain Name between 4 and 32 characters

Figure 7 Switch Admin Module

With the exception of switch time, information displayed in the Switch Admin module is not updated by Advanced Web Tools. To update the information displayed in the Switch Admin module, see "Refreshing the switch Admin Module" on page 37.

△ **CAUTION:** Any changes you make in the Switch Admin module are in a buffered environment and are not applied to the switch until you save the changes. (The exception to this is the License tab, where changes are applied immediately and there is no Apply button, and the upload trace function in the Trace tab.) If you close the Switch Admin module without saving your changes, your changes are lost. To save the buffered changes you make in the Switch Admin module to the switch, click **Apply** before closing the module or before switching to another tab.

Some of the management tasks for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director are performed through the Hi Avail module. This module and the associated tasks are described in"Administering high availability" on page 49.

You can also use telnet commands to perform management tasks. See "Launching the telnet window" on page 37 for information on how to launch a telnet window through Advanced Web Tools.

The remainder of this section describes basic Switch Admin module procedures that are useful for many switch-management operations.

Launching the switch Admin Module

Most of the management procedures in this chapter are performed from the Switch Admin module.

Accessing the Switch Admin module

1. Select a switch from the Fabric Tree.

   The selected switch appears in the Switch View.

2. Click the **Admin** button on the Switch View.

   The Switch Admin module is displayed (as shown in Figure 7 on page 36).

Refreshing the switch Admin Module

To refresh the fabric element information displayed at any time, click the **Refresh** button in any tabbed page of the Switch Admin module.

When you click a different tab in the Switch Admin module, the information in the newly selected tab is refreshed.

Launching the telnet window

When you launch a telnet window for the Core Switch 2/64, SAN Director 2/128, or 4/256 SAN Director, the launch is on a logical-switch basis. This means that for each logical switch, you must launch a separate telnet window. See the *HP StorageWorks Fabric OS 5.x command reference guide* for information about the telnet commands.

NOTE: Advanced Web Tools does not support telnet on the Mozilla browser. You must use an external CLI if using Mozilla.

Telnet access to a switch and the Telnet button in Advanced Web Tools are both disabled when secure mode is enabled for a fabric. You must use `sectelnet` or `SSH` to access the Fabric OS CLI in a secure fabric. These capabilities are not accessible from Advanced Web Tools. For more information on `sectelnet` or `SSH`, see the *HP StorageWorks Secure Fabric OS administrator guide*.

Accessing telnet through Advanced Web Tools

1. Select a switch from the Fabric Tree.

   The selected switch appears in the Switch View.
2. Click the **Telnet** button on the Switch View.

   The Telnet window opens.
3. To close the session when you are done, issue the `exit` command at the telnet prompt.

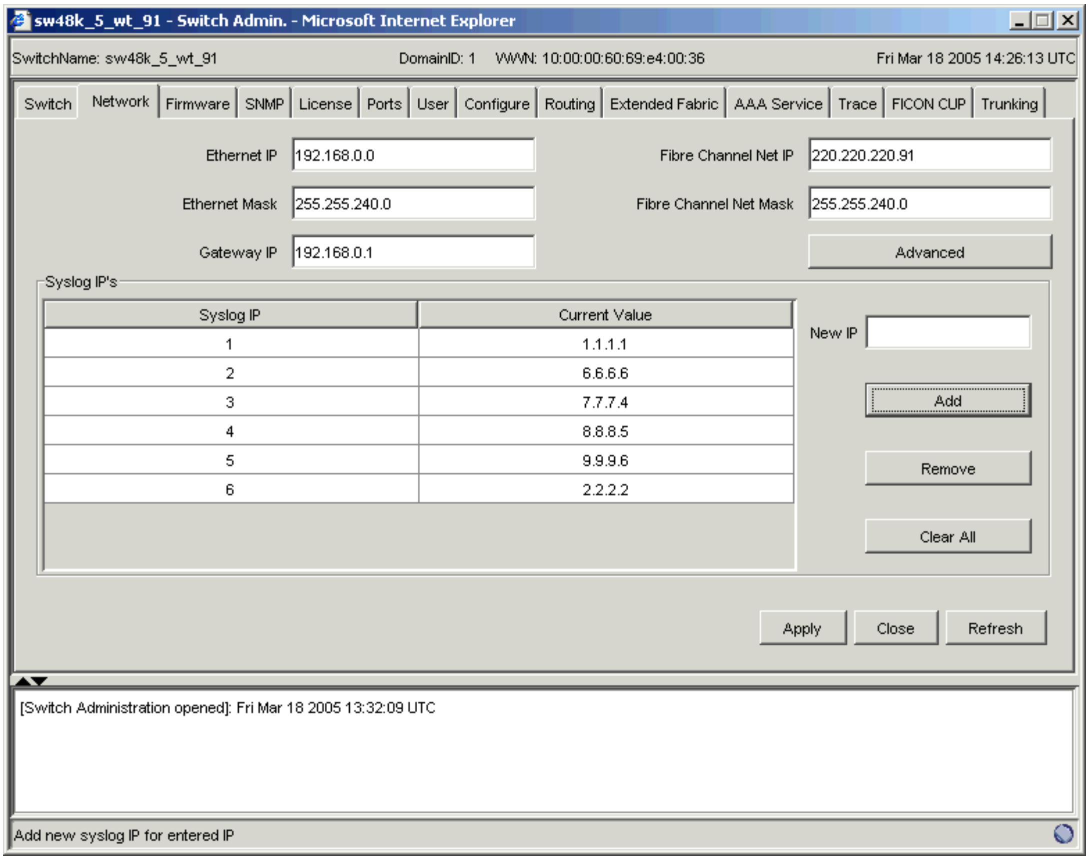
Configuring IP and netmask information

When you configure IP address and netmask information for the Core Switch 2/64, SAN Director 2/128, or 4/256 SAN Director, the configuration is on a logical-switch basis. This means that for each logical switch, you must configure IP and subnet mask information individually.

When changing the Ethernet IP/netmask, the Gateway IP, or the Fibre Channel net IP/netmask from Advanced Web Tools, there is a normal loss of network connection to the switch. If the IP properties have changed, you must close all current windows and restart Advanced Web Tools with the new IP address.

Configuring IP and netmask information

1. Launch the Switch Admin module as described in "Launching the switch Admin Module" on page 36.
2. Click the **Network** tab (see Figure 8).
3. Enter a new value in the appropriate field (for example, `10.77.77.77`).
4. For the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director only:
   - **a.** Click **Advanced**.
   - **b.** Enter a valid IP addresses for the Ethernet IP addresses and subnet mask for CP0 and CP1.
   - **c.** Click **OK** to return to the Network tab.
5. Click **Apply**.
6. Exit and relaunch Advanced Web Tools to continue working.



SwitchName: sw48k_5_wt_91 DomainID: 1 WWN: 10:00:00:60:69:e4:00:36 Fri Mar 18 2005 14:26:13 UTC

Ethernet IP: 192.168.0.0

Ethernet Mask: 255.255.240.0

Gateway IP: 192.168.0.1

Fibre Channel Net IP: 220.220.220.91

Fibre Channel Net Mask: 255.255.240.0

Syslog IP	Current Value
1	1.1.1.1
2	6.6.6.6
3	7.7.7.4
4	8.8.8.5
5	9.9.9.6
6	2.2.2.2

```
[Switch Administration opened]: Fri Mar 18 2005 13:32:09 UTC
```

Add new syslog IP for entered IP

Figure 8 Network tab

Configuring a syslog IP address

The syslog IP address represents the IP address of the server that is running the syslog process. The syslog daemon reads and forwards system messages to the appropriate log files and/or users, depending on the system configuration. When one or more IP addresses are configured, the switch forwards all error log entries to the syslog on the specified servers. Up to six servers are supported. See the *HP StorageWorks Fabric OS 5.x administrator guide* for more information on configuring the syslog daemon.

When you configure a syslog IP address for the Core Switch 2/64 or for a SAN Director 2/128 or 4/256 SAN Director configured with two logical switches, it is on a logical-switch basis. This means that for each logical switch, you must configure a syslog IP address individually.

Configuring the syslog IP address

1. Launch the Switch Admin module as described on page 36.
2. Click the **Network** tab (see Figure 8).
3. Enter a valid IP address in the New IP field (for example, `10.77.77.77`).
4. Click **Add**.

   The configured IP is displayed in the Syslog IP window.
5. Click **Apply**.

Removing a syslog IP address

1. Launch the Switch Admin module as described on page 36.
2. Click the **Network** tab.
3. Select a syslog IP from the table.
4. Click **Remove**.
5. Optional: Click **Clear All** to remove all of the syslog IP addresses.
6. Click **Apply**.

Configuring a switch

Use the Switch tab of the Switch Admin module to perform basic switch configuration. Figure 7 on page 36 shows an example of the Switch tab.

Enabling and disabling a switch

You can identify if a switch is enabled or disabled in the Switch Admin module by looking at the bottom right corner: the ● icon means that the switch is enabled, and the ⊘ icon means that the switch is disabled.

Use the following procedure to enable or disable a switch.

Enabling or disabling a switch

1. Launch the Switch Admin module as described on page 36.
2. Click the **Switch** tab.
3. Select the **Enable** radio button in the Switch Status section to enable the switch, or select the **Disable** radio button to disable the switch.
4. Click **Apply**.

Changing the switch name

Switches can be identified by IP address, domain ID, WWN, or customized switch names that are unique and meaningful.

Switch names can be a maximum of 15 characters long for Fabric OS 5.0.1. They must begin with an alpha character, but otherwise can consist of any combination of alphanumeric and underscore characters.

Changing the switch name

1. Launch the Switch Admin module as described on page 36.
2. Click the **Switch** tab.
3. Enter a new name in the Name field.
4. Click **Apply**.

NOTE: Beginning with Fabric OS 4.4.0, HP recommends that you customize the chassis name for each switch. Some system messages identify a switch service by chassis name, so if you assign meaningful chassis names in addition to meaningful switch names, logs will be more useful. You change the chassis name using the CLI. See the *HP StorageWorks Fabric OS 5.x administrator guide* for instructions on changing the chassis name.

Changing the switch domain ID

Although domain IDs are assigned dynamically when a switch is enabled, you can request a specific ID to resolve a domain ID conflict when you merge fabrics.

1. Launch the Switch Admin module as described on page 36.
2. Disable the switch, as described in "Enabling and disabling a switch."
3. Click the **Switch** tab.
4. Enter a new domain ID in the Domain ID field.

   The domain ID is an integer between 1 and 239.
5. Click **Apply**.
6. Enable the switch, as described in "Enabling and disabling a switch."

Viewing and printing a switch report

The switch report includes the following information:

- A list of switches in the fabric
- Switch configuration parameters
- A list of ISLs and ports
- Name Server information
- Zoning information
- SFP serial ID information

Viewing or printing a switch report

1. Launch the Switch Admin module as described on page 36.
2. Click the **Switch** tab.
3. Click **View Report**.
   A switch report is displayed in a new window.
4. View or print the report using your browser.

Rebooting a switch

When you reboot the switch, the reboot takes effect immediately.

Performing a fast boot

A fast boot reduces boot time significantly by bypassing power-on self test (POST).

1. Launch the Switch Admin module as described on page 36.
2. Click the **Firmware** tab (see Figure 8 on page 38).
3. Select the **Fastboot** radio button.
4. Click **Apply**.

Performing a switch reboot

Use the following procedure to reboot the CP and execute the normal power-on booting sequence.

1. Launch the Switch Admin module as described on page 36.
2. Click the **Firmware** tab (see Figure 8 on page 38).
3. Select the **Reboot** radio button.
4. Click **Apply**.

Changing system configuration parameters

When you change system configuration parameters for the Core Switch 2/64 or for a SAN Director 2/128 or 4/256 SAN Director configured with two logical switches, the change is made on a logical-switch basis. This means that for each logical switch, you must change the system configuration parameters individually.

You must disable the switch before you can configure fabric parameters.

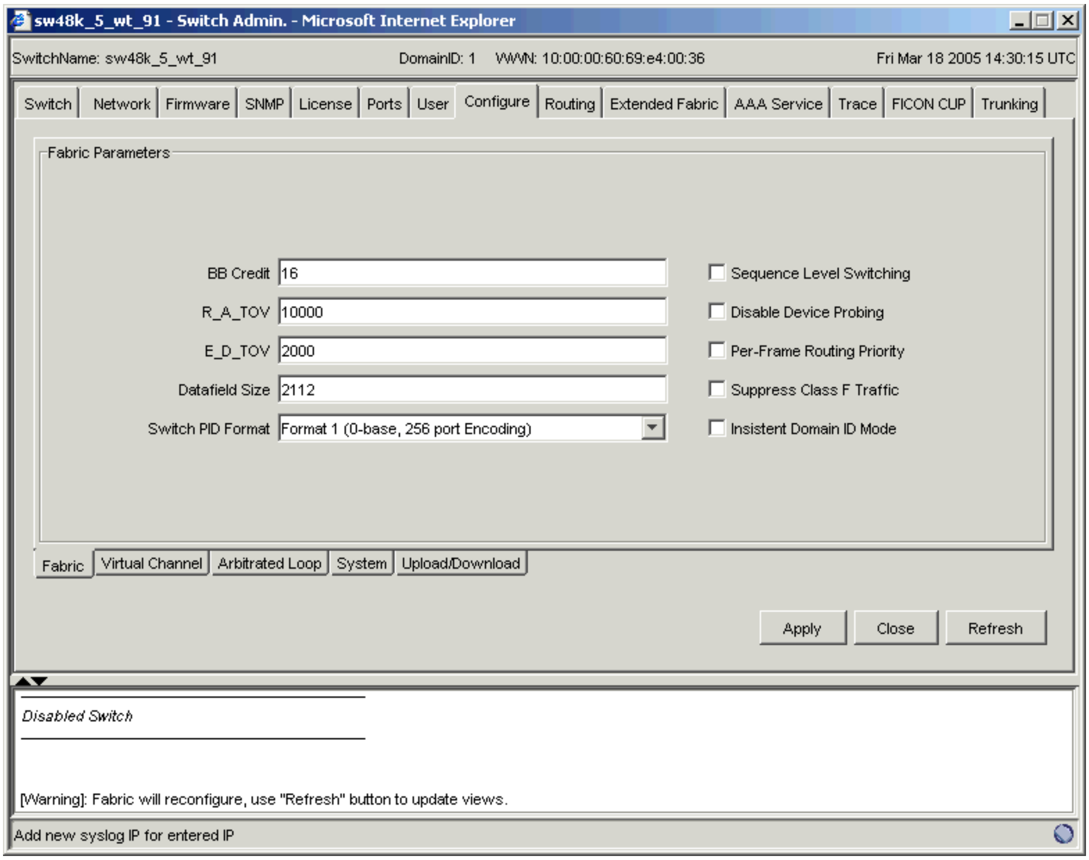
You can change the following system configuration parameters:

- Switch fabric settings
- Virtual channel settings
- Arbitrated loop parameters
- System services

Configuring fabric parameters

You can configure the following fabric parameters using the Configure tab and Fabric subtab of the Switch Admin module (as shown in Figure 9):

- BB Credit, which is the number of buffers available to attached devices for frame receipt. The default BB Credit is 16. The range is 1 through 27.
- R_A_TOV, which is the resource allocation timeout value (in milliseconds). This variable works with the E_D_TOV to determine switch actions when presented with an error condition. The default is 10000. The possible range is 4000 through 120000.
- E_D_TOV, which is the error detect timeout value (in milliseconds). This timer is used to flag a potential error condition when an expected response is not received within the set time. The valid range is 1000 through 5000.
- Datafield size, which is the largest possible datafield size (in bytes). The valid range is 256 through 2112.
- Switch PID Format, which selects a switch PID format from one of the following:
  - Format 1 (0-base, 256 encoding)
  - Format 2 (16-base, 256 encoding)
- Sequence Level Switching: Check this box to enable frames of the same sequence from a particular group to be transmitted together. When this option is not selected, frames are transmitted interleaved among multiple sequences. Under normal circumstances, sequence-level switching should be disabled for better performance. However, some host adapters have issues when receiving interleaved frames among multiple sequences.
- Disable Device Probing: Set this mode only if the switch N_Port discovery process (PLOGI, PRLI, INQUIRY) causes an attached device to fail. When set, devices that do not register with the Name Server are not present in the Name Server database.
- Per-Frame Routing Priority: Choose to select or deselect per-frame routing priority. When enabled, the virtual channel ID is used in conjunction with a frame header to form the final virtual channel ID.
- Suppress Class F Traffic: Applies only if VC-encoded address mode is also set. When checked, translative addressing (which allows private devices to communicate with public devices) is disabled.
- Insistent Domain ID Mode: Set this mode to make the current domain ID insistent across reboots, power cycles, and failovers. This mode is required fabric wide to transmit FICON data.



SwitchName: sw48k_5_wt_91 DomainID: 1 WWN: 10:00:00:60:69:e4:00:36 Fri Mar 18 2005 14:30:15 UTC

BB Credit 16

R_A_TOV 10000

E_D_TOV 2000

Datafield Size 2112

Switch PID Format Format 1 (0-base, 256 port Encoding)

□ Sequence Level Switching

□ Disable Device Probing

□ Per-Frame Routing Priority

□ Suppress Class F Traffic

□ Insistent Domain ID Mode

Disabled Switch

[Warning]: Fabric will reconfigure, use "Refresh" button to update views.

Add new syslog IP for entered IP

Figure 9 Configure tab, Fabric subtab

Configuring fabric parameters

1. Launch the Switch Admin module as described on page 36.
2. Disable the switch as described in ”Enabling and disabling a switch” on page 39.
3. Click the **Configure** tab.
4. Click the **Fabric** subtab.
5. Make the fabric parameter configuration changes.
6. Click **Apply**.
7. Enable the switch as described in ”Enabling and disabling a switch” on page 39.

Enabling insistent domain ID mode (FICON only)

When insistent domain ID (ID_ID) mode is enabled, the current domain setting for the switch is insistent; that is, the same ID is requested during switch reboots, power cycles, CP failovers, firmware downloads, and fabric reconfigurations. If the fabric does not assign the insistent domain ID, the switch segments from the fabric.

This parameter is for use with FICON only.

1. Launch the Switch Admin module as described on page 36.
2. Disable the switch as described in ”Enabling and disabling a switch” on page 39.
3. Click the **Configure** tab.
4. Click the **Fabric** subtab.
5. Check the **Insistent Domain ID Mode** check box.
6. Click **Apply**.
7. Enable the switch as described in ”Enabling and disabling a switch” on page 39.

Configuring virtual channel settings

You can configure the parameters for eight virtual channels to enable fine-tuning for a specific application. You cannot modify the first two virtual channels, which are reserved for switch internal functions.

△ **CAUTION:** The default virtual channel settings have already been optimized for switch performance. Changing the default values can improve switch performance but can also degrade performance. Do not change these settings without fully understanding the effects of the changes.

VC Priority specifies the class of frame traffic given priority for a virtual channel.

Configuring system services

1. Launch the Switch Admin module as described on page 36.
2. Disable the switch as described on page 39.
3. Click the **Virtual Channel** subtab.
4. Enter a value in the **VC Priority** field you want to change. Valid values for all fields are 2 or 3.
5. Click **Apply**.
6. Enable the switch as described on page 39.

Configuring arbitrated loop parameters

You can configure the following arbitrated loop parameters using the Configure tab and Arbitrated Loop subtab of the Switch Admin module:

Send Fan Frames	Check this box to specify that fabric address notification (FAN) frames are sent to public loop devices to notify them of their node ID and address.
Always Send RSCN	Following the completion of loop initialization, a remote state change notification (RSCN) is issued when FL_Ports detect the presence of new devices or the absence of pre-existing devices. Check this box to issue an RSCN upon completion of loop initialization, regardless of the presence or absence of new or pre-existing devices.
Do Not Allow AL_PA 0x00	Check this box to disable 0x00 as an arbitrated loop physical address (AL_PA) value.

Configuring arbitrated loop parameters

1. Launch the Switch Admin module as described on page 36.
2. Disable the switch as described in "Enabling and disabling a switch" on page 39.
3. Select the **Configure** tab.
4. Select the **Arbitrated Loop** subtab.
5. Select or clear the boxes to enable or disable the corresponding arbitrated loop parameters.
6. Click **Apply**.
7. Enable the switch as described in "Enabling and disabling a switch" on page 39.

Configuring system services

You can configure the following system services:

rstatd	Dynamically enables or disables a server that returns system operation information through remote procedures calls (RPC).
rapid	Allows or disallows the API to communicate with the switch.
rusersd	Dynamically enables or disables a server that returns information about the user logged into the system through remote procedure calls (RPC).
Disable RLS Probing	Enables or disables FCP read link status (RLS) information probing for F_Ports and FL_Ports. It is disabled by default.

Configuring system services

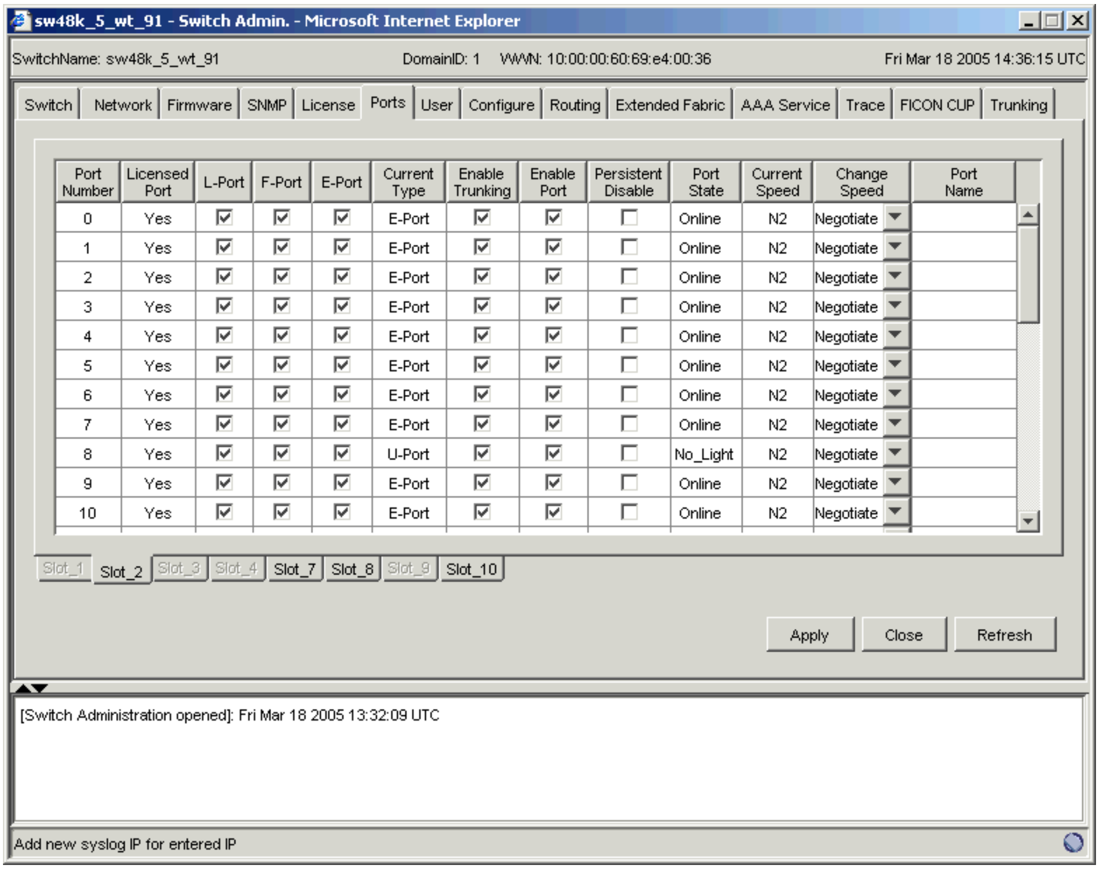
1. Launch the Switch Admin module as described on page 36.
2. Disable the switch as described in ”Enabling and disabling a switch” on page 39.
3. Click the **Configure** tab.
4. Click the **System** subtab.
5. Select the boxes next to the system services that you want to enable. Clear a box to disable a service.

NOTE: Selecting the Disable RLS Probing box disables RLS probing. Clearing this box enables RLS probing.

6. Click **Apply**.
7. Enable the switch as described in ”Enabling and disabling a switch” on page 39.

Configuring ports

Use the Ports tab of the Switch Admin module to perform the basic port configuration procedures described in this section. Figure 10 shows an example of the Ports tab.



SwitchName: sw48k_5_wt_91 DomainID: 1 WWN: 10:00:00:60:69:e4:00:36 Fri Mar 18 2005 14:36:15 UTC

Port Number	Licensed Port	L-Port	F-Port	E-Port	Current Type	Enable Trunking	Enable Port	Persistent Disable	Port State	Current Speed	Change Speed	Port Name
0	Yes	☑	☑	☑	E-Port	☑	☑	□	Online	N2	Negotiate	
1	Yes	☑	☑	☑	E-Port	☑	☑	□	Online	N2	Negotiate	
2	Yes	☑	☑	☑	E-Port	☑	☑	□	Online	N2	Negotiate	
3	Yes	☑	☑	☑	E-Port	☑	☑	□	Online	N2	Negotiate	
4	Yes	☑	☑	☑	E-Port	☑	☑	□	Online	N2	Negotiate	
5	Yes	☑	☑	☑	E-Port	☑	☑	□	Online	N2	Negotiate	
6	Yes	☑	☑	☑	E-Port	☑	☑	□	Online	N2	Negotiate	
7	Yes	☑	☑	☑	E-Port	☑	☑	□	Online	N2	Negotiate	
8	Yes	☑	☑	☑	U-Port	☑	☑	□	No_Light	N2	Negotiate	
9	Yes	☑	☑	☑	E-Port	☑	☑	□	Online	N2	Negotiate	
10	Yes	☑	☑	☑	E-Port	☑	☑	□	Online	N2	Negotiate	

[Switch Administration opened]: Fri Mar 18 2005 13:32:09 UTC

Add new syslog IP for entered IP

Figure 10 Ports tab

Configuring port type

The Current Type column in the Ports tab indicates the actual or current type of the port:

- If the port is offline, this value is the allowed types or U-Port, if no type constraint has been specified.
- If the port is online, this value is the type the port has actually negotiated to (normally L-Port for storage ports, F-Port for HBA or host ports, and E-Port for ISLs).

The L-Port, F-Port, and E-Port columns indicate any constraints on what types the port can negotiate to when it comes up.

Use the following procedure to configure the port type.

Configuring the port type

1. Launch the Switch Admin module as described on page 36.
2. Click the **Ports** tab.
3. Perform the following, according to switch type:
   - For Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, select the subtab that corresponds to the correct slot for the logical switch.
   - For 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, 4Gb SAN Switch for HP p-Class BladeSystem, and SAN Switch 4/32, proceed directly to the next step.
4. Select a port by clicking the port number.
5. Clear the following check boxes, depending on how you want to configure the port type:
   - L-Port: The port can be used to connect a loop device.
   - F-Port: The port can be used to connect a non-loop device.
   - E-Port: The port can be used to connect to another switch.

   By default, all of these boxes are selected, meaning that there is no constraint on port type. The port negotiates to its preferred type when the switch comes up, depending on what type of device or switch it is attached to.

   Clearing a check box guarantees that the port does not attempt to function as a port of the cleared type.

   At least one type must remain selected. L-Port and F-Port cannot both be cleared.
6. Click **Apply**.

Configuring port speed

The Current Speed column in the Ports tab indicates the current speed of the port. Use the following procedure to change the port speed.

1. Launch the Switch Admin module as described on page 36.
2. Click the **Ports** tab.
3. Perform the following, according to switch type:
   - For Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, select the subtab that corresponds to the correct slot for the logical switch.
   - For 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, 4Gb SAN Switch for HP p-Class BladeSystem, and SAN Switch 4/32, proceed directly to the next step.
4. Select a port speed from the Change Speed drop-down list corresponding to the port for which you want to change the speed.
5. Click **Apply**.

Assigning a name to a port

Port names are optional. You can assign a name to a port to make port grouping easier. The Port Name column in the **Ports** tab displays the port name, if one exists.

Naming a port

1. Launch the Switch Admin module as described on page 36.
2. Click the **Ports** tab.
3. Perform the following, according to switch type:
   - For Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, select the slot subtab that corresponds to the correct slot for the logical switch.
   - For 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, 4Gb SAN Switch for HP p-Class BladeSystem, and SAN Switch 4/32, proceed directly to the next step.
4. Double-click the Port Name field for the port you want to change.
5. Enter a name for the port. Port names can be from 0 through 32 alphanumeric characters. HP recommends unique part names, although they are not required.
6. Click **Apply**.

Disabling a port over reboots

Use the following procedure to disable a port so that it remains disabled if the switch reboots.

Disabling a port so that it remains disabled over reboots

1. Launch the Switch Admin module as described on page 36.
2. Click the **Ports** tab.
3. Perform the following, according to switch type:
   - For Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, select the slot subtab that corresponds to the correct slot for the logical switch.
   - For 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, 4Gb SAN Switch for HP p-Class BladeSystem, and SAN Switch 4/32, proceed directly to the next step.
4. Select the **Persistent Disable** check box for the port you want to keep disabled over reboots.
5. Click **Apply**.

Enabling and disabling a port

All licensed ports are enabled by default. You can disable and reenable them as necessary.

If a port is not licensed you cannot enable it until you install the Ports on Demand license. (See Activating Ports on Demand for more information.) The Licensed Port column indicates whether a port is licensed.

NOTE: If you disable a principal ISL port (an ISL port that is used to communicate with the principal switch), the fabric reconfigures. If the port was connected to a device, that device is no longer accessible from the fabric. For more information, see the *HP StorageWorks Fabric OS 5.x administrator guide*.

Enabling or disabling a port

1. Launch the Switch Admin module as described on page 36.
2. Click the **Ports** tab.
3. Perform the following, according to switch type:
   - For Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, select the slot subtab that corresponds to the correct slot for the logical switch.
   - For 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, 4Gb SAN Switch for HP p-Class BladeSystem, and SAN Switch 4/32, proceed directly to the next step.

4. Select the box in the Enable Port column that corresponds to the port you want to enable, or clear the box in the Enable Port column that corresponds to the port you want to disable.
5. Click **Apply**.
6. Review the log at the bottom of the tab for information regarding the switch configuration changes.

Activating Ports on Demand

The 4/8 SAN Switch and 4/16 SAN Switch can be purchased with 8, 12, or 16 licensed ports. The SAN Switch 4/32 can be purchased with 16 or 32 licensed ports. As your needs increase, you can activate unlicensed ports by purchasing and installing the HP StorageWorks 4- or 8-port upgrade license.

By default, ports 0 through 7 are enabled on the 4/8 SAN Switch and 4/16 SAN Switch, and ports 0 through 15 are enabled on the SAN Switch 4/32. By installing a Port Upgrade License, you can enable an additional 4 ports on the 4/8 SAN Switch and an additional 8 ports on the SAN Switch 4/32. You can install up to two Port Upgrade Licenses on each switch.

For each switch model, Table 7 shows the ports that are enabled by default and the ports that can be enabled after you install the first and second Port Upgrade Licenses.

Table 7 Ports enabled with Ports on Demand licenses

Enabled ports	**4/8 and 4/16 SAN Switch**	**SAN Switch 4/32**
Ports enabled without Port Upgrade License (default)	0–7	0–15
Ports enabled when you install first Port Upgrade License	8–11	16–23
Ports enabled when you install second Port Upgrade License	12–15	24–31

Once you have installed the license keys, you must enable the ports. You can do so without disrupting switch operation, as described in "Enabling and disabling a port" on page 46. Alternatively, you can disable and reenable the switch to activate all ports as described in "Enabling and disabling a switch" on page 39.

To unlock a Ports on Demand license, you can either use the supplied license key or generate a license key. If you need to generate a key, launch an Internet browser and go to the HP licensing web site at http://webkey.external.hp.com/welcome.asp. Select **Generate a license key** and follow the instructions to generate the key.

Enabling a Port Upgrade License

1. Launch the Switch Admin module as described on page 36.
2. Click the **Ports** tab.

   In the Ports tab, the Licensed Port column indicates whether the port is licensed or not.
3. Install the Port Upgrade License.

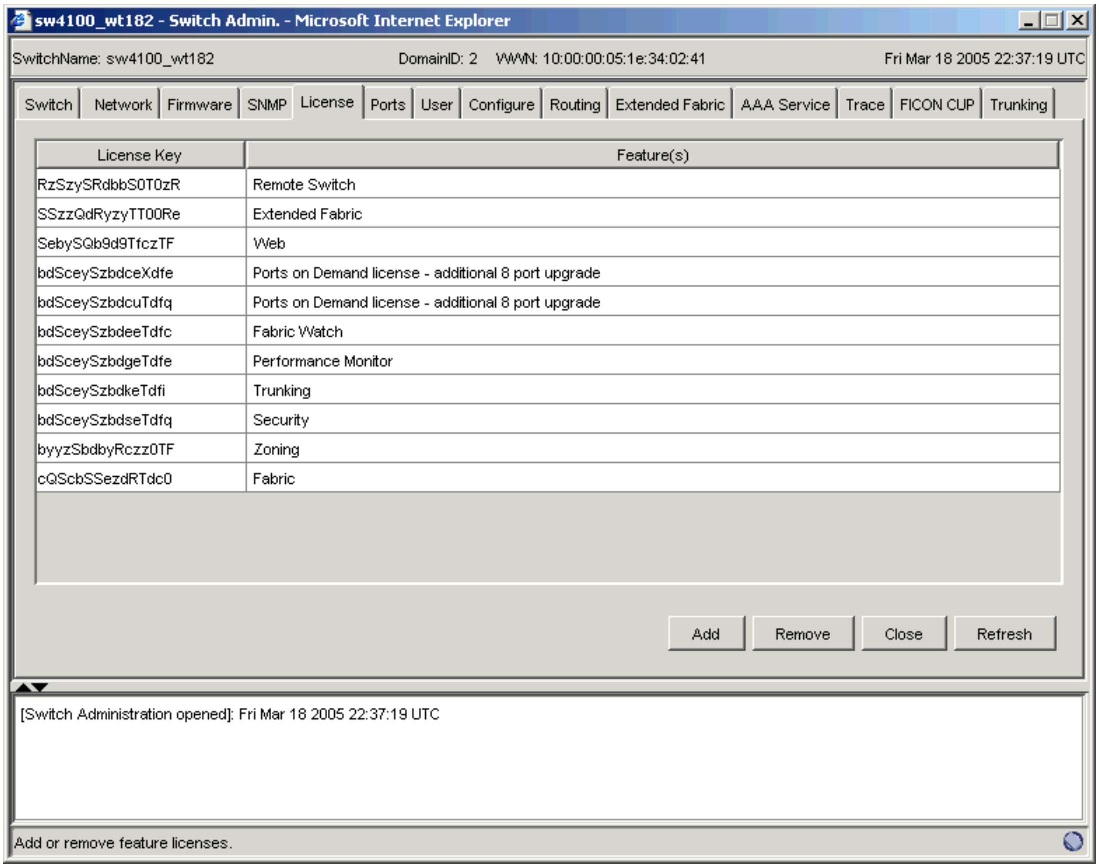
   For instructions, see "Maintaining licensed features."
4. Enable the ports, as described in "Enabling and disabling a port" on page 46.

If you remove a Port Upgrade License, the licensed ports become disabled after the next platform reboot or the next port deactivation.

Maintaining licensed features

Feature licenses might be supplied with switch software, or you can purchase licenses separately from your switch vendor, who will provide you with keys to unlock the features. License keys are provided on a per-chassis basis, so for products that support multiple logical switches (domains), a license key applies to all domains within the chassis.

The licensed features currently installed on the switch are listed in the License tab of the Switch Admin module, as shown in Figure 11. If the feature is listed, it is installed and immediately available. When you enable some licenses, such as ISL Trunking, you might need to change the state of the port to enable the feature on the link.



sw4100_wt182 - Switch Admin. - Microsoft Internet Explorer

SwitchName: sw4100_wt182 DomainID: 2 WWN: 10:00:00:05:1e:34:02:41 Fri Mar 18 2005 22:37:19 UTC

License Key	Feature(s)
RzSzySRdbbS0T0zR	Remote Switch
SSzzQdRyzyTT00Re	Extended Fabric
SebySQb9d9TfczTF	Web
bdSceySzbdceXdfe	Ports on Demand license - additional 8 port upgrade
bdSceySzbdcuTdfq	Ports on Demand license - additional 8 port upgrade
bdSceySzbdeeTdfc	Fabric Watch
bdSceySzbdgeTdfe	Performance Monitor
bdSceySzbdkeTdfi	Trunking
bdSceySzbdseTdfq	Security
byyzSbdbyRczz0TF	Zoning
cQScbSSezdRTdc0	Fabric

[Switch Administration opened]: Fri Mar 18 2005 22:37:19 UTC

Add or remove feature licenses.

Figure 11 License tab

Activating a license on a switch

Before you can unlock a licensed feature, you must obtain a license key by visiting the HP licensing web site at http://webkey.external.hp.com/welcome.asp. Select **Generate a license key** and follow the instructions to generate the key.

1. Launch the Switch Admin module as described on page 36.
2. Click the **License** tab.
3. Click **Add**.

   The Add License dialog box opens.
4. Paste or enter a license key in the box.
5. Click **Add License**.
6. Click **Refresh** to display the new licenses in the License tab.

NOTE: Some licenses (for example, ISL Trunking) do not take effect until the switch is rebooted.

Removing a license from a switch

△ **CAUTION:** Removing the Advanced Web Tools license from a switch makes that switch unavailable from Advanced Web Tools. If you remove the Advanced Web Tools license from a Core Switch 2/64, SAN Director 2/128, or 4/256 SAN Director, both logical switches are then unavailable from Advanced Web Tools.

1. Launch the Switch Admin module as described on page 36.
2. Click the **License** tab.

3. Click the license you want to remove.
4. Click **Remove**.

Administering high availability

The procedures in this section apply only to the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, because the HA module is available only on these switch types. See the *HP StorageWorks Fabric OS 5.x administrator guide* for additional information about HA.

Launching the High Availability module

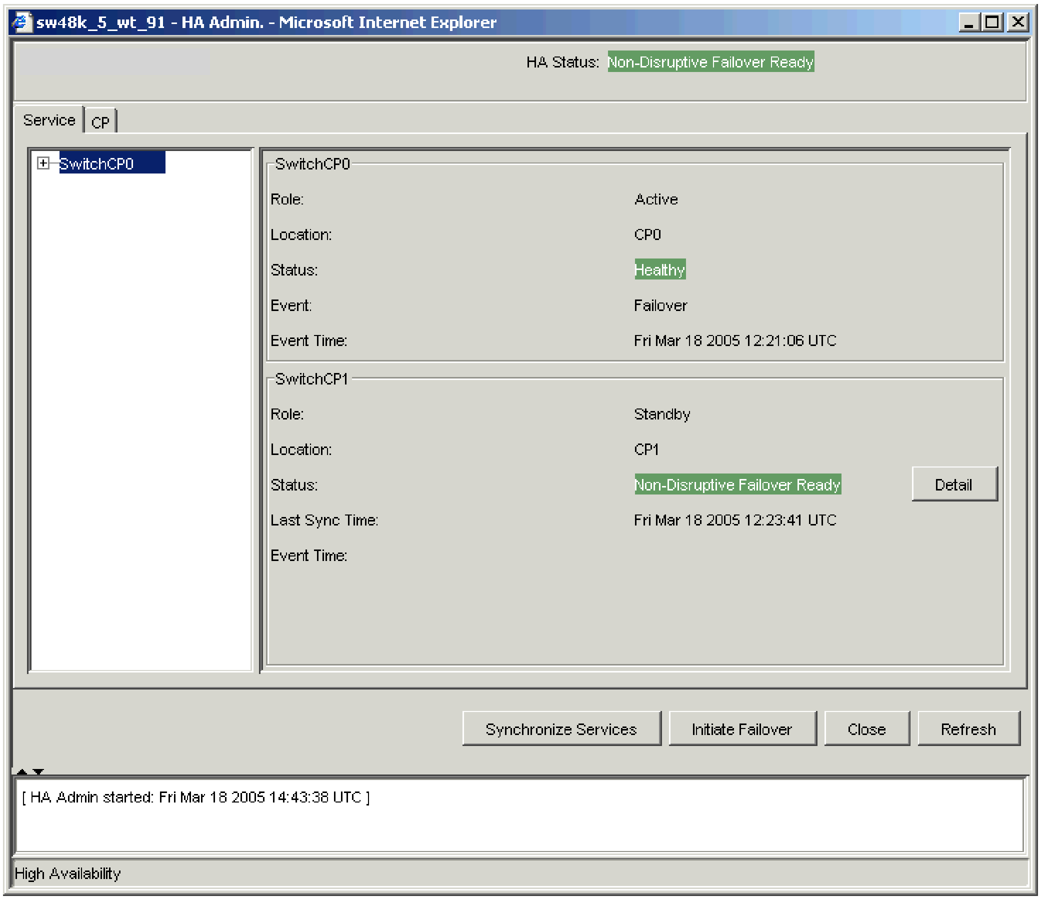
The background color of the Hi Avail button indicates the overall status of the switch. The High Availability module displays information about the status of the HA feature on the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director and each CP. It also enables you to perform tasks such as CP failover or to synchronize services on the CPs.

To launch the High Availability module

1. Select a Core Switch 2/64, SAN Director 2/128, or 4/256 SAN Director from the Fabric Tree.

   The selected director appears in the Switch View.
2. Click the **Hi Avail** button on the Switch View.

   The HA Admin module is displayed, as shown in Figure 12.


sw48k_5_wt_91 - HA Admin. - Microsoft Internet Explorer

HA Status: Non-Disruptive Failover Ready

SwitchCP0

Role: Active

Location: CP0

Status: Healthy

Event: Failover

Event Time: Fri Mar 18 2005 12:21:06 UTC

SwitchCP1

Role: Standby

Location: CP1

Status: Non-Disruptive Failover Ready

Last Sync Time: Fri Mar 18 2005 12:23:41 UTC

Event Time:

[HA Admin started: Fri Mar 18 2005 14:43:38 UTC]

Figure 12 High availability mode

Note that there is a background color with the HA Status for each CP. The HA Admin module is not refreshed.

3. Click **Refresh** to update the information displayed in the HA Admin module.

Synchronizing services on the CP

A nondisruptive CP failover is possible only when all the services on it have been synchronized.

1. Launch the Hi Avail module as described in "Launching the High Availability module" on page 49.
2. If the HA Status box displays `Non-Disruptive Failover Ready`, you are done.

   If the HA Status box displays `Disruptive Failover Ready`, continue with step 3.
3. Click the **Synchronize Services** button.

   The Warning dialog box opens.
4. Click **Yes** and wait for the CPs to complete a synchronization of services, so that a nondisruptive failover is ready.
5. Click **Refresh** to update the HA Status box.

   When the HA Status box displays `Non-Disruptive Failover Ready`, a failover can be initiated without disrupting frame traffic on the fabric.

Initiating a CP failover

A nondisruptive failover might take about 30 seconds to complete. During the failover, the Advanced Web Tools session and associated windows are invalidated. You must close all Advanced Web Tools windows and relaunch Advanced Web Tools.

To initiate a CP failover

1. Launch the Hi Avail module as described in "Launching the High Availability module" on page 49.
2. Verify that the HA Status box displays `Non-Disruptive Failover Ready or Disruptive Failover Ready`. See Synchronizing services on the CP for more information.
3. Click **Initiate Failover**.

   The Warning dialog box opens.
4. Click **Yes** to initiate a non-disruptive failover.
5. When prompted, close the Advanced Web Tools Switch Explorer window and all associated windows, and relaunch Advanced Web Tools.

Monitoring events

Advanced Web Tools displays fabric-wide and switch-wide events. Event information includes sortable fields for the following:

- Switch name
- Message number
- Time stamp
- Indication that the event is from a logical switch or a chassis
- Severity level
- Unique message identifier (in the form *`moduleID-messageType`*)
- Detailed error message for root cause analysis

There are four message severity levels: Critical, Error, Warning, and Info. Table 8 lists the event message severity levels displayed in the Switch Events and Fabric Events windows, and explains what qualifies event messages to be certain levels.

In both the Switch Events window and the Fabric Events window, you can click the Filter button to launch the Filter Events dialog box. The Filter Events dialog box allows you to define which events should be displayed in the Switch Events window or Fabric Events window. For more information on filtering events, see "Filtering fabric and switch events" on page 53.

Table 8 Event severity levels

Icon and level	Description
❗ Critical (1)	Critical-level messages indicate that the software has detected serious problems that will eventually cause a partial or complete failure of a subsystem if not corrected immediately. For example, a power supply failure or rise in temperature must receive immediate attention.
⚠ Error (2)	Error-level messages represent an error condition that does not significantly affect overall system functionality. For example, error-level messages might indicate timeouts on certain operations, failures of certain operations after retries, invalid parameters, or failure to perform a requested operation.
⚠ Warning (3)	Warning-level messages highlight a current operating condition that should be checked or it might lead to a failure in the future. For example, a power supply failure in a redundant system relays a warning that the system is no longer operating in redundant mode and that the failed power supply needs to be replaced or fixed.
ℹ Info (4)	Information-level messages report the current nonerror status of the system components, for example, the online and offline status of a fabric port.

Displaying fabric events

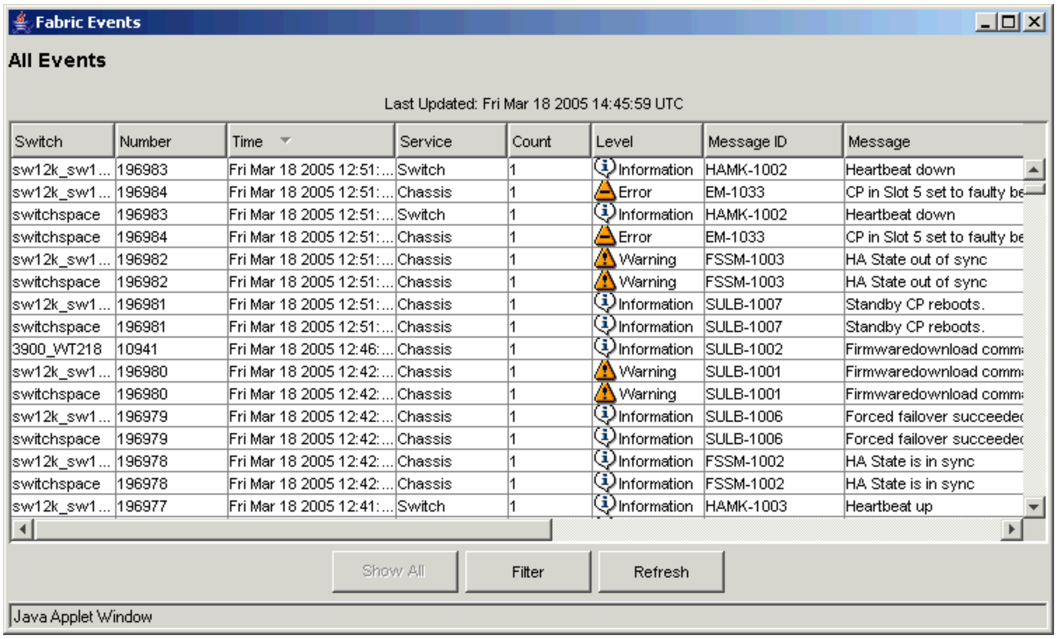
Events are displayed for all switches in the fabric in the Fabric Events window (see Figure 13). Fabric events are not polled. You must click Refresh from the Fabric Events window to poll fabric events. Switch events are polled every 15 seconds.

Fabric Events can be collected only for switches that have the same security level (http or https) as the launch switch. For switches that have a different level of security from the launch switch, a message is displayed at the top of the window indicating how many switches have no events reported from the last polling. For detailed information on the switch names and reasons for not polling (if available), click **Details**.

To display fabric events

1. Click a fabric from the Fabric Tree.
2. Click the **Fabric Events** icon on the Fabric Toolbar.
   The Fabric Events window is displayed (see Figure 13).
3. Optional: Click the column head to sort the events by a particular column.
   Drag the column divider to resize a column.

You can also filter events, as described in "Filtering fabric and switch events" on page 53.



All Events

Last Updated: Fri Mar 18 2005 14:45:59 UTC

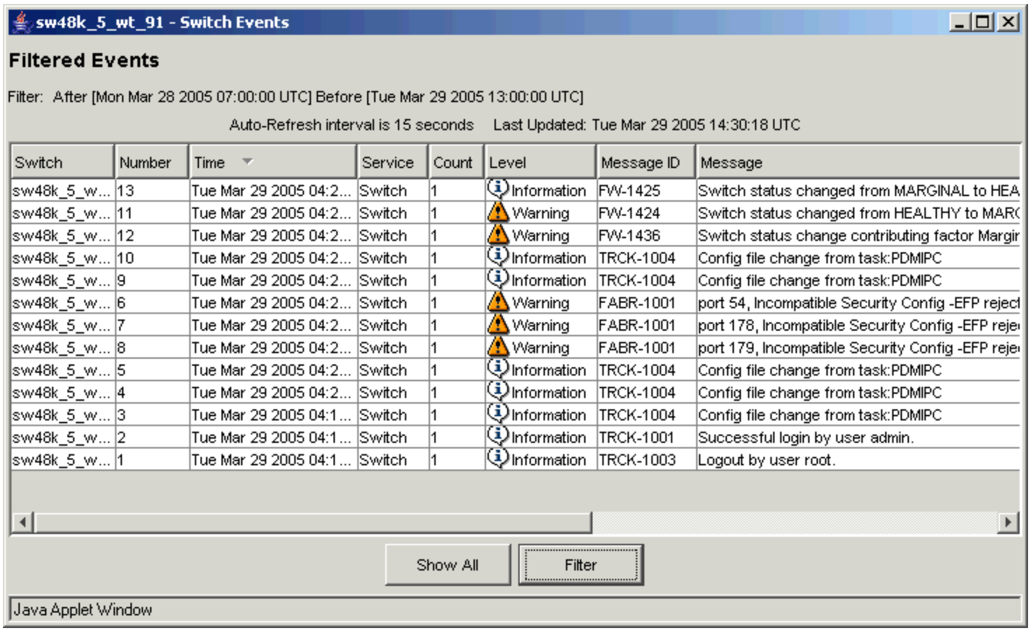
Switch	Number	Time	Service	Count	Level	Message ID	Message
sw12k_sw1...	196983	Fri Mar 18 2005 12:51:...	Switch	1	Information	HAMK-1002	Heartbeat down
sw12k_sw1...	196984	Fri Mar 18 2005 12:51:...	Chassis	1	Error	EM-1033	CP in Slot 5 set to faulty be
switchspace	196983	Fri Mar 18 2005 12:51:...	Switch	1	Information	HAMK-1002	Heartbeat down
switchspace	196984	Fri Mar 18 2005 12:51:...	Chassis	1	Error	EM-1033	CP in Slot 5 set to faulty be
sw12k_sw1...	196982	Fri Mar 18 2005 12:51:...	Chassis	1	Warning	FSSM-1003	HA State out of sync
switchspace	196982	Fri Mar 18 2005 12:51:...	Chassis	1	Warning	FSSM-1003	HA State out of sync
sw12k_sw1...	196981	Fri Mar 18 2005 12:51:...	Chassis	1	Information	SULB-1007	Standby CP reboots.
switchspace	196981	Fri Mar 18 2005 12:51:...	Chassis	1	Information	SULB-1007	Standby CP reboots.
3900_WT218	10941	Fri Mar 18 2005 12:46:...	Chassis	1	Information	SULB-1002	Firmwaredownload comm
sw12k_sw1...	196980	Fri Mar 18 2005 12:42:...	Chassis	1	Warning	SULB-1001	Firmwaredownload comm
switchspace	196980	Fri Mar 18 2005 12:42:...	Chassis	1	Warning	SULB-1001	Firmwaredownload comm
sw12k_sw1...	196979	Fri Mar 18 2005 12:42:...	Chassis	1	Information	SULB-1006	Forced failover succeeded
switchspace	196979	Fri Mar 18 2005 12:42:...	Chassis	1	Information	SULB-1006	Forced failover succeeded
sw12k_sw1...	196978	Fri Mar 18 2005 12:42:...	Chassis	1	Information	FSSM-1002	HA State is in sync
switchspace	196978	Fri Mar 18 2005 12:42:...	Chassis	1	Information	FSSM-1002	HA State is in sync
sw12k_sw1...	196977	Fri Mar 18 2005 12:41:...	Switch	1	Information	HAMK-1003	Heartbeat up

Figure 13 Fabric Events window

Displaying switch events

The Switch Events window displays a running log of events for the selected switch (see Figure 14). Switch events are polled and updated every 15 seconds, so there is no refresh-on-demand option for switch events, as there is for the fabric events.

For two-switch configurations, all chassis-related events are displayed in the event list of each logical switch for convenience.



Filtered Events

Filter: After [Mon Mar 28 2005 07:00:00 UTC] Before [Tue Mar 29 2005 13:00:00 UTC]

Auto-Refresh interval is 15 seconds Last Updated: Tue Mar 29 2005 14:30:18 UTC

Switch	Number	Time	Service	Count	Level	Message ID	Message
sw48k_5_w...	13	Tue Mar 29 2005 04:2...	Switch	1	Information	FW-1425	Switch status changed from MARGINAL to HEA
sw48k_5_w...	11	Tue Mar 29 2005 04:2...	Switch	1	Warning	FW-1424	Switch status changed from HEALTHY to MAR(
sw48k_5_w...	12	Tue Mar 29 2005 04:2...	Switch	1	Warning	FW-1436	Switch status change contributing factor Margir
sw48k_5_w...	10	Tue Mar 29 2005 04:2...	Switch	1	Information	TRCK-1004	Config file change from task:PDMIPC
sw48k_5_w...	9	Tue Mar 29 2005 04:2...	Switch	1	Information	TRCK-1004	Config file change from task:PDMIPC
sw48k_5_w...	6	Tue Mar 29 2005 04:2...	Switch	1	Warning	FABR-1001	port 54, Incompatible Security Config -EFP reject
sw48k_5_w...	7	Tue Mar 29 2005 04:2...	Switch	1	Warning	FABR-1001	port 178, Incompatible Security Config -EFP reje
sw48k_5_w...	8	Tue Mar 29 2005 04:2...	Switch	1	Warning	FABR-1001	port 179, Incompatible Security Config -EFP reje
sw48k_5_w...	5	Tue Mar 29 2005 04:2...	Switch	1	Information	TRCK-1004	Config file change from task:PDMIPC
sw48k_5_w...	4	Tue Mar 29 2005 04:2...	Switch	1	Information	TRCK-1004	Config file change from task:PDMIPC
sw48k_5_w...	3	Tue Mar 29 2005 04:1...	Switch	1	Information	TRCK-1004	Config file change from task:PDMIPC
sw48k_5_w...	2	Tue Mar 29 2005 04:1...	Switch	1	Information	TRCK-1001	Successful login by user admin.
sw48k_5_w...	1	Tue Mar 29 2005 04:1...	Switch	1	Information	TRCK-1003	Logout by user root.

Figure 14 Switch Events window

Displaying switch events

1. Click the switch from the Fabric Tree.

   The Switch View opens.
2. Click the **Events** button on the Switch View.

   The Switch Events window is displayed (see Figure 14 on page 52).
3. Optional: Click the column head to sort the events by a particular column. Drag the column divider to resize a column.

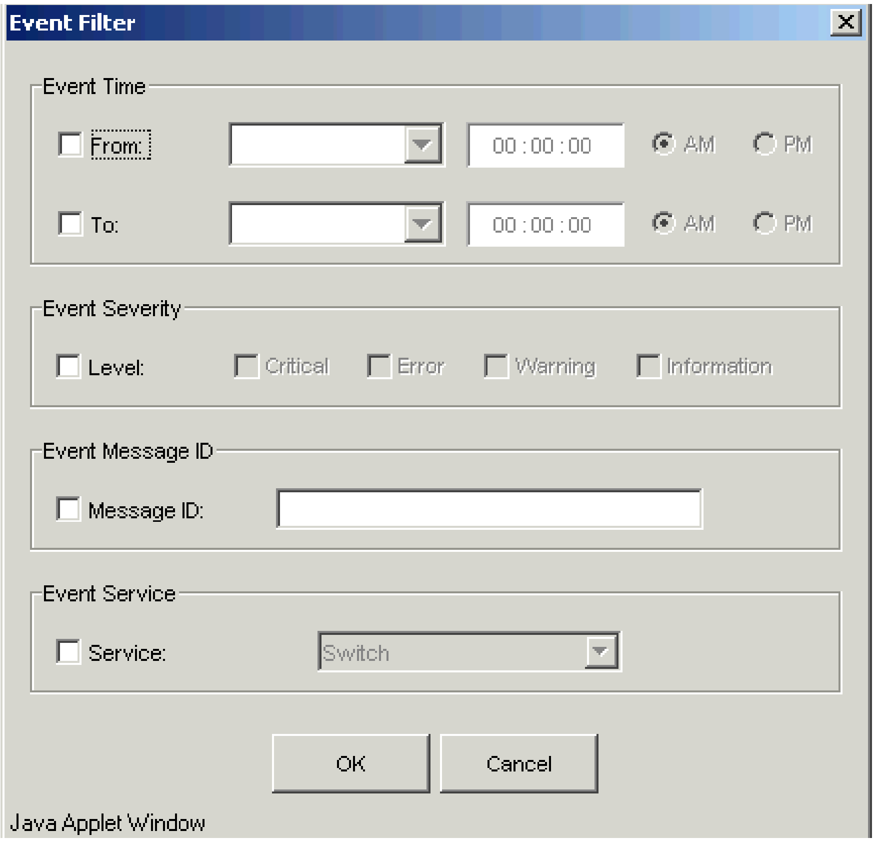
You can also filter events, as described in Filtering fabric and switch events next.

Filtering fabric and switch events

You can filter the events in the Fabric Events window and Switch Events window by time, severity, message ID, and service. You can apply either one type of filter at a time or multiple types of filters at the same time. The Switch Events and Fabric Events windows both have a Filter button. Click the **Filter** button to display the Event Filter dialog box (see Figure 15).

When a filter is applied, the Show All button is active in the events window and the type of filter applied is identified at the top of the events window (see Figure 14 on page 52). To unapply a filter, click the **Show All** button in the events window.

NOTE: For two-switch configurations, clicking the Events button for a given switch filters out switch service events from the other switch. Chassis service is shown in both events lists.



Event Filter

Event Time

□ From: 00 : 00 : 00 ● AM ○ PM

□ To: 00 : 00 : 00 ● AM ○ PM

Event Severity

□ Level: □ Critical □ Error □ Warning □ Information

Event Message ID

□ Message ID:

Event Service

□ Service: Switch

Figure 15 Event Filter dialog box

Filtering events by time intervals

1. Launch the Fabric Events or Switch Events window as described in "Displaying fabric events" on page 51 and "Displaying switch events" on page 52.
2. Click **Filter**.

   The Event Filter dialog box opens.

3. To filter events within a certain time period:
   a. Click **From** and enter the start time and date in the boxes.
   b. Click **To** and enter the finish time and date in the boxes.
4. To filter all events beginning at a certain date and time, click **From** and enter the start time and date in the boxes.
5. To filter events up until a certain date and time, click **To** and enter the finish time and date in the boxes.
6. Click **OK**.

The filter is enabled and the enabled filter type is displayed in the events window.

Filtering events by event severity levels

1. Launch the Fabric or Switch Events window as described in "Displaying fabric events" on page 51 or "Fabric Events window" on page 52.
2. Click **Filter**.

   The Event Filter dialog box opens.
3. Click **Level**.

   The event severity level check boxes are enabled.
4. Click the event levels you want to display.
5. Click **OK**.

   The filter is enabled and the enabled filter type is displayed in the events window.

Filtering events by message ID

1. Launch the Fabric Events or Switch Events window as described in "Displaying fabric events" on page 51 or "Fabric Events window" on page 52.
2. Click **Filter**.

   The Event Filter dialog box opens.
3. Click **Message ID**.
4. Enter the message IDs in the associated box.

   You can enter multiple message IDs as long as you separate them by commas. You can enter either the full message ID (`moduleID-messageType`) or a partial ID (`moduleID` only).
5. Click **OK**.

   The filter is enabled and the enabled filter type is displayed in the events window.

Filtering events by service component

1. Launch the Fabric Events or Switch Events window as described in "Displaying fabric events" on page 51 or "Fabric Events window" on page 52.
2. Click **Filter**.

   The Event Filter dialog box opens.
3. Click **Service**.

   The event service drop-down list is enabled.
4. Select either **Switch** or **Chassis** from the drop-down list to show only those messages from the logical switch or from the chassis.
5. Click **OK**.

   The filter is enabled and the enabled filter type is displayed in the events window.

Displaying a fabric topology report

A fabric topology report lists all of the domains in the fabric and the active paths for each domain. A sample fabric topology report is shown in Figure 16.

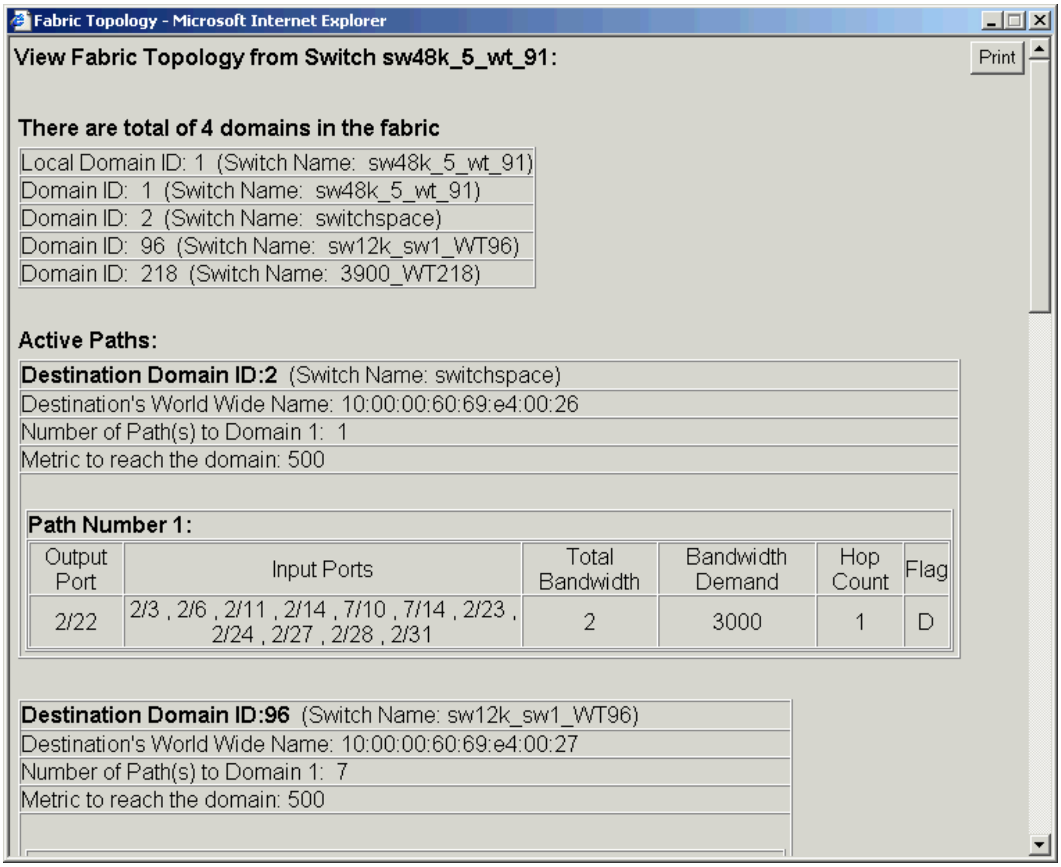
Viewing a fabric topology report

1. Click the **Fabric Topology** icon on the Fabric Toolbar.

   The Fabric Topology window opens.

2. Click the **Print** button to print a topology report.

   A Print button is located at the top and bottom of the report. Both Print buttons have the same function.



View Fabric Topology from Switch sw48k_5_wt_91:

There are total of 4 domains in the fabric

Local Domain ID: 1 (Switch Name: sw48k_5_wt_91)
Domain ID: 1 (Switch Name: sw48k_5_wt_91)
Domain ID: 2 (Switch Name: switchspace)
Domain ID: 96 (Switch Name: sw12k_sw1_WT96)
Domain ID: 218 (Switch Name: 3900_WT218)

Active Paths:

Destination Domain ID:2 (Switch Name: switchspace)
Destination's World Wide Name: 10:00:00:60:69:e4:00:26
Number of Path(s) to Domain 1: 1
Metric to reach the domain: 500

Path Number 1:

Output Port	Input Ports	Total Bandwidth	Bandwidth Demand	Hop Count	Flag
2/22	2/3 , 2/6 , 2/11 , 2/14 , 7/10 , 7/14 , 2/23 , 2/24 , 2/27 , 2/28 , 2/31	2	3000	1	D

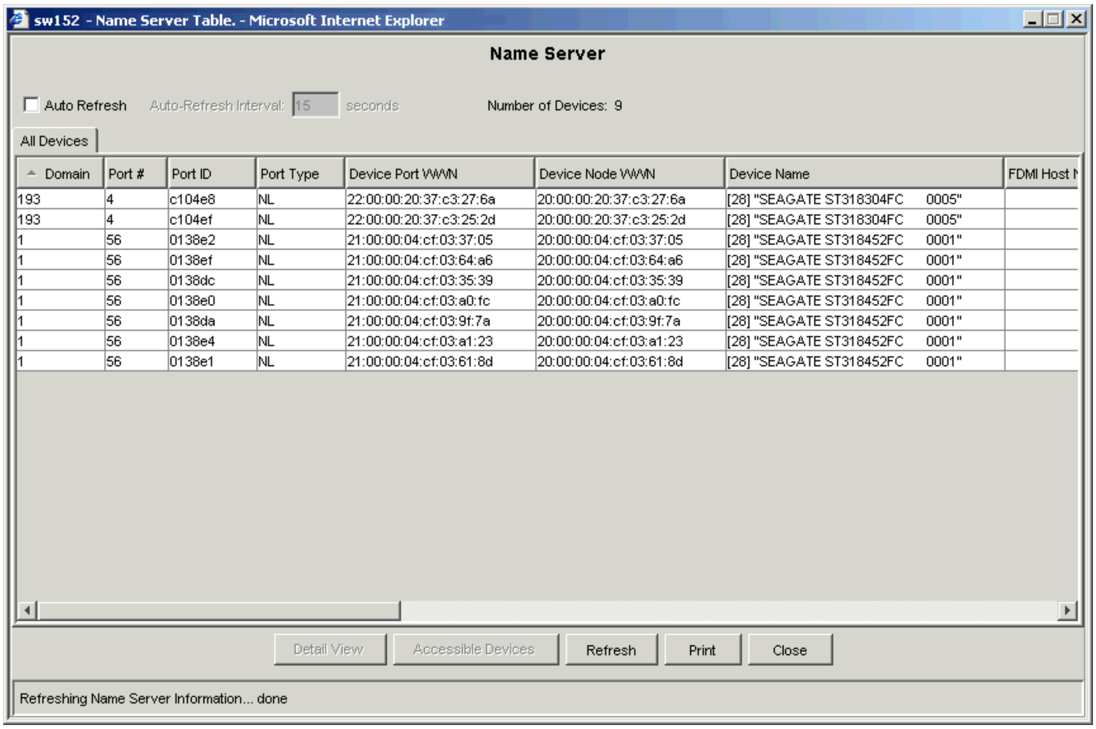
Destination Domain ID:96 (Switch Name: sw12k_sw1_WT96)
Destination's World Wide Name: 10:00:00:60:69:e4:00:27
Number of Path(s) to Domain 1: 7
Metric to reach the domain: 500

Figure 16 Fabric topology report

Displaying the Name Server entries

Advanced Web Tools displays Name Server entries listed in the Simple Name Server database (see Figure 17). This includes all Name Server entries for the fabric, not only those related to the local domain. Each row in the table represents a different device.

NOTE: Name Server entries are not polled by default. Click **Refresh** in the Name Server window to poll Name Server entries. You can also click the **Auto Refresh** check box and specify a time interval at which the Name Server entries will be refreshed.



□ Auto Refresh Auto-Refresh Interval: 15 seconds Number of Devices: 9

Domain	Port #	Port ID	Port Type	Device Port WWN	Device Node WWN	Device Name	FDMI Host
193	4	c104e8	NL	22:00:00:20:37:c3:27:6a	20:00:00:20:37:c3:27:6a	[28] "SEAGATE ST318304FC 0005"	
193	4	c104ef	NL	22:00:00:20:37:c3:25:2d	20:00:00:20:37:c3:25:2d	[28] "SEAGATE ST318304FC 0005"	
1	56	0138e2	NL	21:00:00:04:cf:03:37:05	20:00:00:04:cf:03:37:05	[28] "SEAGATE ST318452FC 0001"	
1	56	0138ef	NL	21:00:00:04:cf:03:64:a6	20:00:00:04:cf:03:64:a6	[28] "SEAGATE ST318452FC 0001"	
1	56	0138dc	NL	21:00:00:04:cf:03:35:39	20:00:00:04:cf:03:35:39	[28] "SEAGATE ST318452FC 0001"	
1	56	0138e0	NL	21:00:00:04:cf:03:a0:fc	20:00:00:04:cf:03:a0:fc	[28] "SEAGATE ST318452FC 0001"	
1	56	0138da	NL	21:00:00:04:cf:03:9f:7a	20:00:00:04:cf:03:9f:7a	[28] "SEAGATE ST318452FC 0001"	
1	56	0138e4	NL	21:00:00:04:cf:03:a1:23	20:00:00:04:cf:03:a1:23	[28] "SEAGATE ST318452FC 0001"	
1	56	0138e1	NL	21:00:00:04:cf:03:61:8d	20:00:00:04:cf:03:61:8d	[28] "SEAGATE ST318452FC 0001"	

Refreshing Name Server Information... done

Figure 17 Name server window

Viewing a list of the switches in the Name Server

1. Click the **Name Server** icon ▦ on the Fabric Toolbar.

   The Name Server Table is displayed.

2. Optional: Check the **Auto Refresh** check box on the Name Server window. Enter an auto-refresh interval (in seconds); the minimum (and default) interval is 15 seconds.

   The Name Server entries refresh at the rate you set.

Printing the Name Server entries

1. Click the **Name Server** icon ▦ on the Fabric Toolbar.

   The Name Server Table is displayed.

2. Click **Print**.

   The Page Setup dialog box opens.

3. Make changes, as appropriate.
4. Click **OK** in the Page Setup dialog box.

   The Print dialog box opens.

5. Select a printer and click **OK** in the Print dialog box.

Displaying detailed Name Server information for a particular device

1. Click the **Name Server** icon ▦ on the Fabric Toolbar.

   The Name Server Table opens.

2. Click a device in the Domain column.
3. Click **Detail View**.

   The Name Server Information dialog box displays information specific to that device.

Displaying the zone members of a particular device

1. Click the **Name Server** icon ▦ on the Fabric Toolbar.

   The Name Server Table opens.
2. Click a device in the Domain column.
3. Click **Accessible Devices**.

   The Zone Accessible Devices window displays accessible zone member information specific to that device.

Physically locating a switch using beaconing

Use the Beacon button to physically locate a switch in a fabric. The beaconing function helps to physically locate a switch by sending a signal to the specified switch, resulting in an LED light pattern that cycles through all ports for each switch (from left to right).

Enabling beaconing

1. Select a switch from the Fabric Tree.

   The selected switch appears in the Switch View.
2. Click the **Beacon** button on the Switch View.

   The LED lights on the actual switch (selected in the GUI) light up on the physical switch in a pattern running back and forth across the switch itself. The beaconing is not shown in the GUI.
3. Look at the physical switches in your installation location to identify the switch.

Displaying swapped port area IDs

Use this procedure to view swapped ports on the switch. You cannot swap ports using Advanced Web Tools; you can swap ports using the Fabric OS CLI only.

Determining whether a port area ID has been swapped with another switch port

1. Launch the Switch Admin module as described in "Launching the switch Admin Module" on page 36.
2. Click the **Ports** tab.
3. View the Port (Area ID) column in the Port Settings tab.

   For ports that have been swapped, the port number is followed by the area ID, in parentheses.

4 Maintaining configurations and firmware

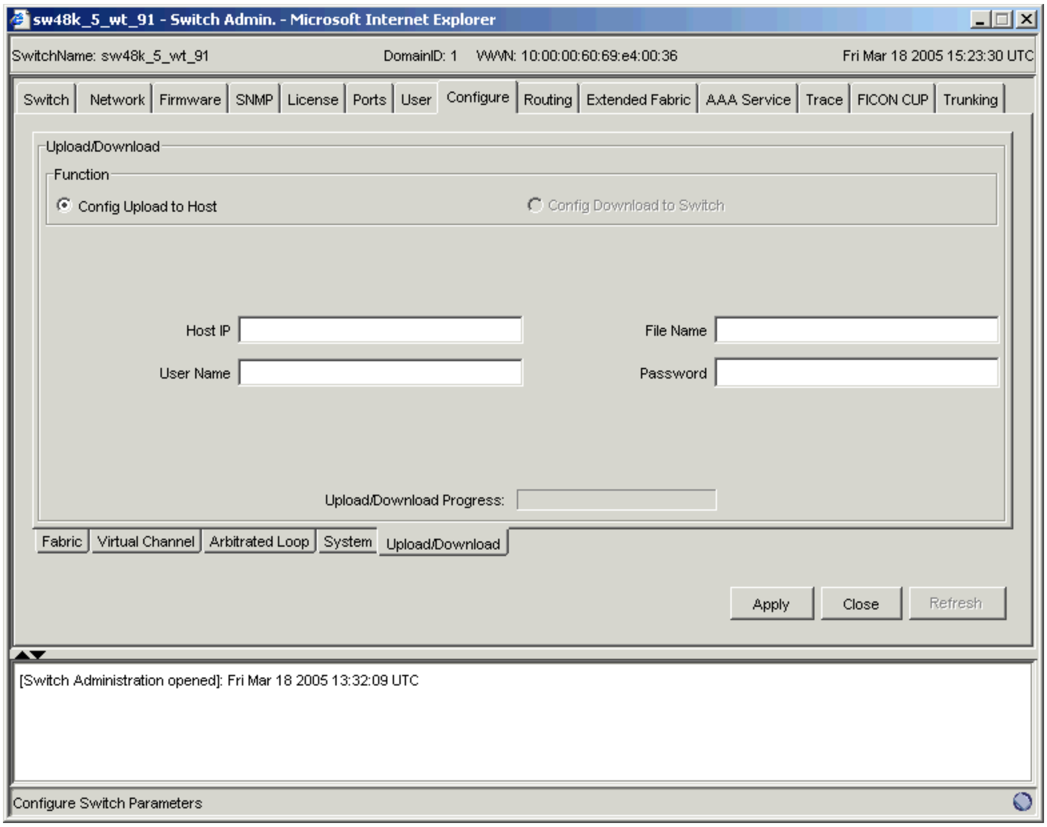
This chapter contains the following information:

- Maintaining configurations, page 59
- Performing a firmware download, page 60

Maintaining configurations

It is important to maintain consistent configuration settings on all switches in the same fabric, because inconsistent parameters (such as inconsistent PID formats) can cause fabric segmentation. As part of standard configuration maintenance procedures, HP recommends that you back up configuration data for every switch on a host computer server for emergency reference.

This section contains procedures for basic switch configuration maintenance. Use the Configure tab and Upload/Download subtab of the Switch Admin module to perform these tasks (see Figure 18).



sw48k_5_wt_91 - Switch Admin. - Microsoft Internet Explorer

SwitchName: sw48k_5_wt_91 DomainID: 1 WWN: 10:00:00:60:69:e4:00:36 Fri Mar 18 2005 15:23:30 UTC

Function: ● Config Upload to Host ○ Config Download to Switch

[Switch Administration opened]: Fri Mar 18 2005 13:32:09 UTC

Figure 18 Configure tab, Upload/Download Subtab

Backing up a configuration file

Keep a backup copy of the configuration file in case the configuration is lost or unintentional changes are made. You should keep individual backup files for all switches in the fabric. You should avoid copying configurations from one switch to another.

When you back up a configuration file for the Core Switch 2/64 or for a SAN Director 2/128 or 4/256 SAN Director configured with two logical switches, the backup is performed on a logical-switch basis. This means that you must back up a separate configuration file for each logical switch.

To back up a configuration file

1. Launch the Switch Admin module as described on page 36.
2. Click the **Configure** tab.
3. Click the **Upload/Download** subtab (see Figure 18).

4. Select the **Config Upload to Host** radio button.
5. Enter the user name, password, and host IP information.
6. Enter the configuration file with a fully qualified path.
7. Click **Apply**.

You can monitor the progress by looking at the Upload/Download Progress bar on the Configure tab.

Restoring a configuration

Restoring a configuration involves overwriting the configuration on the switch by downloading a previously saved backup configuration file. Perform this procedure during a planned down time.

Make sure that the configuration file you are downloading is compatible with your switch model, because configuration files from other model switches might cause your switch to fail.

Downloading a configuration to the switch

1. Launch the Switch Admin module as described on page 36.
2. Disable the switch, as described in "Enabling and disabling a switch" on page 39.

   You can download configurations only to a disabled (offline) switch.
3. Click the **Configure** tab.
4. Click the **Upload/Download** subtab (see Figure 18 on page 59).
5. Select the **Config Download to Switch** radio button.
6. Enter the user name, password, and host IP information.
7. Enter the configuration file with a fully qualified path.
8. Click **Apply**.

   You can monitor the progress by looking at the Upload/Download Progress bar on the Configure tab.
9. Enable the switch, as described in "Enabling and disabling a switch" on page 39.

Performing a firmware download

During a firmware download, the switch reboots and the browser temporarily loses connection with the switch. When the connection is restored, the version of the software running in the browser is different from the new software version that has been installed and activated on the switch. You must close all of the Advanced Web Tools windows and log in again to avoid a firmware version mismatch. Note that for chassis-based switches, you might get pop-up messages that imply the loss of connection is temporary and will soon be resolved. You still need to close all windows and log in again.

When you request a firmware download, the system first checks the file size that is to be downloaded. If the compact flash does not have enough space, Advanced Web Tools displays a message and the download does not occur. If this happens, contact your switch support supplier.

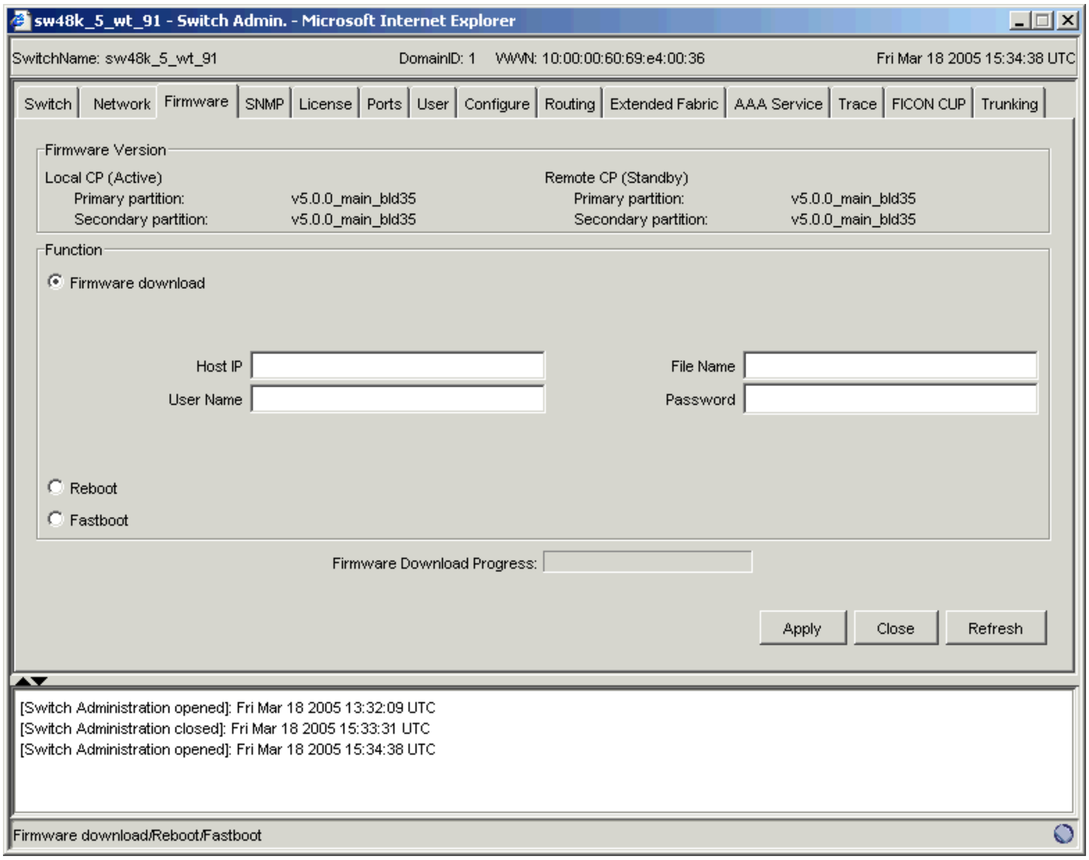
Downloading a new version of the firmware

1. Launch the Switch Admin module as described on page 36.
2. Click the **Firmware** tab (see Figure 19).
3. Select the **Firmware Download** radio button.
4. Enter the host IP address, user name, password, and fully qualified path to the file name.
5. Click **Apply**.

   The firmware download begins. You can monitor the firmware download status on the Firmware Download progress bar.

   About halfway through the download process, connection to the switch is lost and Advanced Web Tools invalidates the current session. (Advanced Web Tools invalidates all windows if upfront login is enabled, but invalidates only the Switch Admin session, if upfront login is not enabled.)
6. Close all Advanced Web Tools windows and log in again.

   If the firmware download is in progress when you log in, you can continue to monitor its progress.



SwitchName: sw48k_5_wt_91 DomainID: 1 WWN: 10:00:00:60:69:e4:00:36 Fri Mar 18 2005 15:34:38 UTC

Firmware Version

Local CP (Active)		Remote CP (Standby)	
Primary partition:	v5.0.0_main_bld35	Primary partition:	v5.0.0_main_bld35
Secondary partition:	v5.0.0_main_bld35	Secondary partition:	v5.0.0_main_bld35

Function

● Firmware download

Host IP
File Name
User Name
Password

○ Reboot

○ Fastboot

Firmware Download Progress:

```
[Switch Administration opened]: Fri Mar 18 2005 13:32:09 UTC
[Switch Administration closed]: Fri Mar 18 2005 15:33:31 UTC
[Switch Administration opened]: Fri Mar 18 2005 15:34:38 UTC
```

Firmware download/Reboot/Fastboot

Figure 19 Firmware tab

5 Configuring standard security features

This chapter contains the following information:

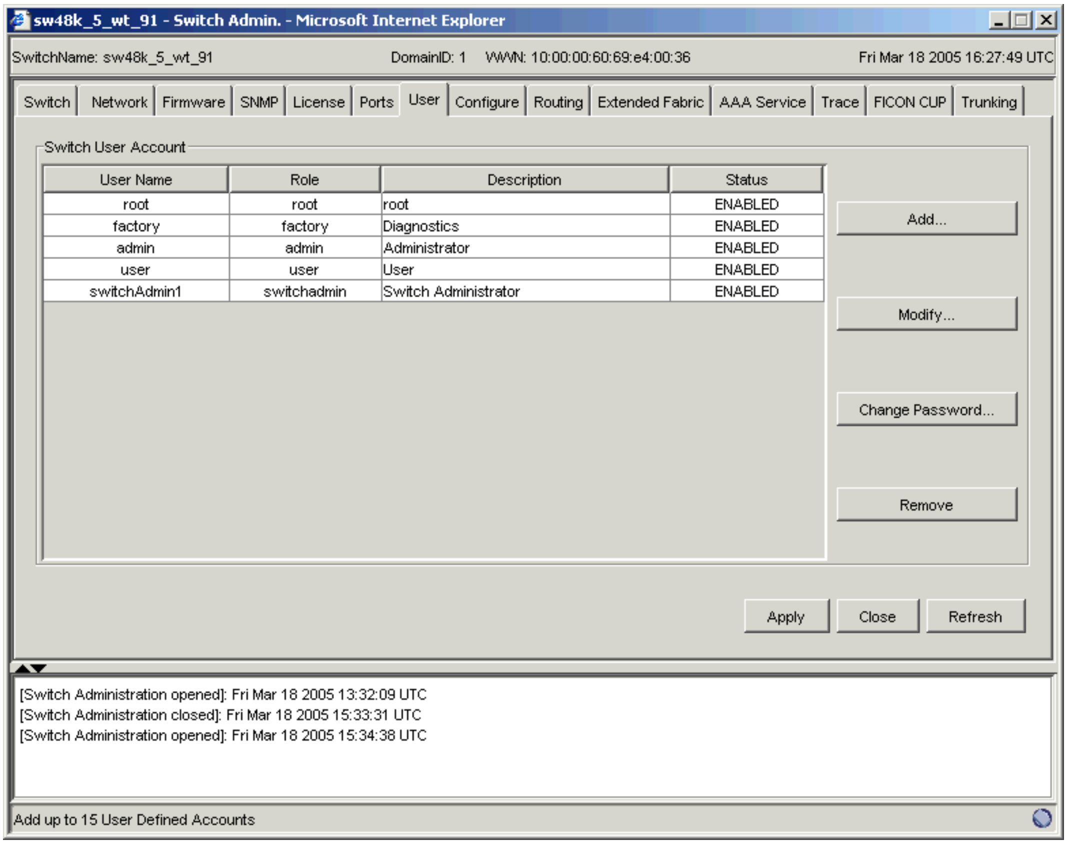
- Creating and maintaining user-defined accounts, page 63
- Configuring SNMP information, page 65
- Managing the RADIUS server, page 67

Creating and maintaining user-defined accounts

In addition to the five default accounts—root, factory, admin, switchAdmin, and user—Fabric OS supports up to 15 user-defined accounts in each logical switch (domain). These accounts expand your ability to track account access and audit administrative activities.

The User tab of the Switch Admin module (see Figure 20) displays account information and enables you to create and manage user accounts, if you are logged in as an admin. If you are logged in as a switchAdmin, you can change your own password but cannot view or modify other accounts. If you are logged in as a user role, you cannot access the Switch Admin module.

NOTE: If you are operating in secure mode, you can perform these operations only on the primary FCS switch.



User Name	Role	Description	Status
root	root	root	ENABLED
factory	factory	Diagnostics	ENABLED
admin	admin	Administrator	ENABLED
user	user	User	ENABLED
switchAdmin1	switchadmin	Switch Administrator	ENABLED

```
[Switch Administration opened]: Fri Mar 18 2005 13:32:09 UTC
[Switch Administration closed]: Fri Mar 18 2005 15:33:31 UTC
[Switch Administration opened]: Fri Mar 18 2005 15:34:38 UTC
```

Figure 20 User tab

Displaying account information

1. Launch the Switch Admin module as described on page 36.
2. Click the **User** tab.

   A list of the default and user-defined accounts is displayed. If you are logged in using the switchAdmin role, only your account information is displayed.

Creating a user-defined account

1. Launch the Switch Admin module as described on page 36.
2. Click the **User** tab.
3. Click the **Add** button.

   The Add User Account dialog box opens.
4. Enter the user name, which must begin with an alphabetic character. The name can be up to 40 characters long. It is case-sensitive and can contain alphabetic and numeric characters, the dot and the underscore. It must be different from all other account names on the logical switch.
5. Select a role from the drop-down list: admin, switchAdmin, or user in nonsecure mode; admin, switchAdmin, user, or nonfcsadmin in secure mode.

   See "Role-based access control" on page 22 for information about these roles.
6. Optional: Enter a description of the account.
7. Select the **Enabled** or **Disabled** radio button to enable or disable the account.
8. Enter the password for the account.

   Passwords can contain 8 to 40 characters. They must begin with an alphabetic character. They can include numeric characters, the dot, and the underscore. Passwords are case-sensitive; they are not displayed when you enter them on the command line.
9. Reenter the password in the Confirm Password field for confirmation.
10. Click **OK**.
11. Click **Apply** to save your changes.

Deleting a user-defined account

1. Launch the Switch Admin module as described on page 36.
2. Click the **User** tab.
3. Select the account to remove.
4. Click the **Remove** button.
5. Click **Apply** to save your changes.

You cannot delete the default accounts. An account cannot delete itself. All active CLI sessions for the deleted account are logged out.

Changing account parameters

1. Launch the Switch Admin module as described on page 36.
2. Click the **User** tab.
3. Select the account to modify.

   You cannot modify the default root and factory accounts, even if you are logged in as root.
4. Click the **Modify** button.

   The Modify User Account dialog box opens. You cannot change the user name of the account. To change the user name, you must delete the account and create a new account.
5. Select a role from the drop-down list: admin, switchAdmin, or user in nonsecure mode; admin, switchAdmin, user, or nonfcsadmin in secure mode.

   You can change the role only on user-level accounts. You cannot change the role on the default accounts. You cannot change the role of your own account.
6. Enter a new description.

   You can change the description only on user-level accounts. You cannot change the description of the default accounts. You cannot change the description of your own account.

7. Select the **Enabled** or **Disabled** radio button to enable or disable the account.

   You can enable and disable user- and admin-level accounts except for your own account. You cannot enable or disable your own account or the factory account. Only the root account can disable itself.

   If you disable an account, all active CLI sessions for that account are logged out.
8. Click **OK**.
9. Click **Apply** to save your changes.

Changing an account password

1. Launch the Switch Admin module as described on page 36.
2. Click the **User** tab.
3. Select the account to modify.

   If you are logged in as admin, you can change the password of your own account, peer admin accounts, switchAdmin accounts, and user accounts. You cannot change the root or factory account passwords.

   If you are logged in as a switchAdmin, you can change the password only on your own account.
4. Click the **Change Password** button.

   The Set User Account Password dialog box opens.

   If you are changing the password of an admin account, you must also provide the current password. You do not need to provide the current password if you are changing the password of a lower-level user account.
5. Enter the current password of the account. This step is required only if you are changing the password of your own or a peer admin account.
6. Enter the new password of the account.

   The new password must have at least one character different from the old password.
7. Reenter the new password in the Confirm Password box.
8. Click **OK**.
9. Click **Apply** to save your changes.

Configuring SNMP information

This section describes how to manage the configuration of the SNMP agent in the switch. The configuration includes SNMPv1 and SNMPv3 configuration, accessControl, and systemGroup configuration parameters.

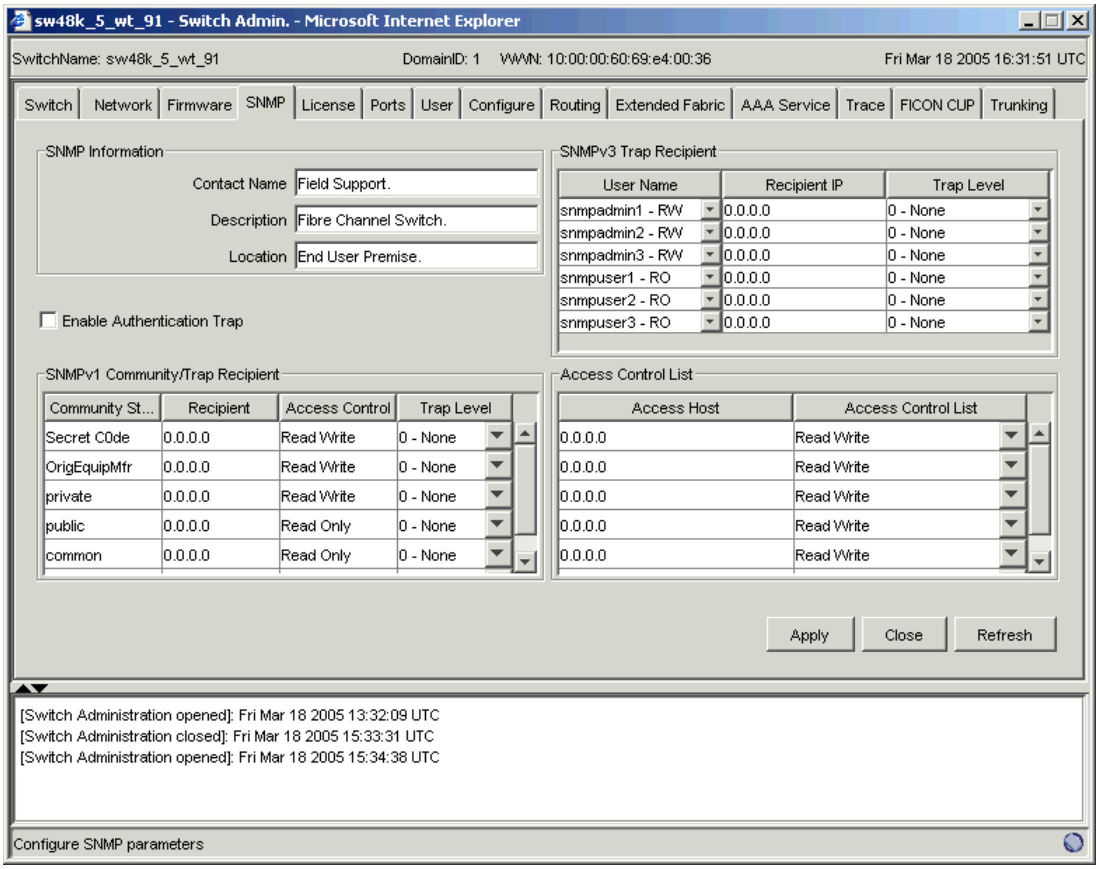
For more information, see the `snmpConfig` command in the *HP StorageWorks Fabric OS 5.x command reference guide*.

Setting SNMP trap levels

When you set trap levels for the Core Switch 2/64 or for a SAN Director 2/128 or 4/256 SAN Director configured with two logical switches, trap levels are set on a logical-switch basis. This means that for each logical switch, you must set trap levels individually.

Setting trap levels

1. Launch the Switch Admin module as described on page 36.
2. Click the **SNMP** tab (see Figure 21).



SwitchName: sw48k_5_wt_91 DomainID: 1 WWN: 10:00:00:60:69:e4:00:36 Fri Mar 18 2005 16:31:51 UTC

SNMP Information

Contact Name: Field Support.

Description: Fibre Channel Switch.

Location: End User Premise.

☐ Enable Authentication Trap

SNMPv3 Trap Recipient

User Name	Recipient IP	Trap Level
snmpadmin1 - RW	0.0.0.0	0 - None
snmpadmin2 - RW	0.0.0.0	0 - None
snmpadmin3 - RW	0.0.0.0	0 - None
snmpuser1 - RO	0.0.0.0	0 - None
snmpuser2 - RO	0.0.0.0	0 - None
snmpuser3 - RO	0.0.0.0	0 - None

SNMPv1 Community/Trap Recipient

Community St...	Recipient	Access Control	Trap Level
Secret C0de	0.0.0.0	Read Write	0 - None
OrigEquipMfr	0.0.0.0	Read Write	0 - None
private	0.0.0.0	Read Write	0 - None
public	0.0.0.0	Read Only	0 - None
common	0.0.0.0	Read Only	0 - None

Access Control List

Access Host	Access Control List
0.0.0.0	Read Write
0.0.0.0	Read Write
0.0.0.0	Read Write
0.0.0.0	Read Write
0.0.0.0	Read Write

```
[Switch Administration opened]: Fri Mar 18 2005 13:32:09 UTC
[Switch Administration closed]: Fri Mar 18 2005 15:33:31 UTC
[Switch Administration opened]: Fri Mar 18 2005 15:34:38 UTC
```

Configure SNMP parameters

Figure 21 SNMP tab

3. Select a trap level for a recipient from the corresponding Trap Level drop-down list in the SNMPv1 and SNMPv3 sections.

   The level you select identifies the minimum event level that prompts a trap.
4. Click **Apply**.

Configuring SNMP information

When you configure SNMP information for the Core Switch 2/64 or for a SAN Director 2/128 or 4/256 SAN Director configured with two logical switches, it is on a logical-switch basis. This means that for each logical switch, you must configure SNMP information individually.

Changing the systemGroup configuration parameters

1. Launch the Switch Admin module as described on page 36.
2. Click the **SNMP** tab (see Figure 21).
3. Enter a contact name, a description, and a location in the SNMP Information section.
4. Optional: Select the **Enable Authentication Trap** check box to allow authentication traps to be sent to the reception IP address.
5. Click **Apply**.

Setting SNMPv1 configuration parameters

1. Launch the Switch Admin module as described on page 36.
2. Click the **SNMP** tab (see Figure 21).
3. Double-click a community string in the SNMPv1 section and enter a new community string.
4. Double-click a recipient IP address in the SNMPv1 section and enter a new IP address.
5. Click **Apply**.

Setting SNMPv3 configuration parameters

1. Launch the Switch Admin module as described on page 36.
2. Select the **SNMP** tab (see Figure 21 on page 66).
3. Select a user name from the User Name drop-down list in the SNMPv3 section.
4. Double-click a recipient IP address in the SNMPv3 section and enter a new IP address.
5. Select a trap level from the Trap Level drop-down list.
6. Click **Apply**.

Changing the accessControl configuration

1. Launch the Switch Admin module as described on page 36.
2. Click the **SNMP** tab (see Figure 21 on page 66).
3. Double-click an access host IP address in the Access Control List section and enter a new host IP address.
4. Select a permission for the host from the Access Control List drop-down list.

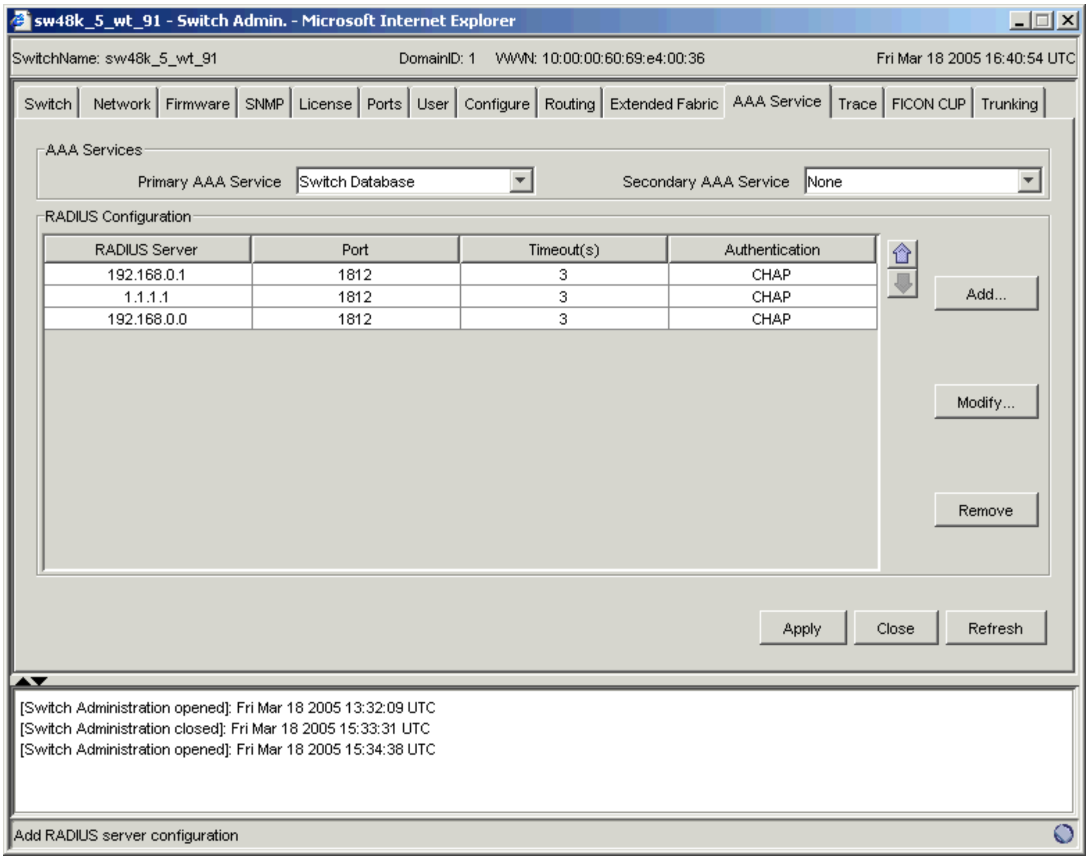
   Options are Read Only and Read Write.
5. Click **Apply**.

Managing the RADIUS server

Fabric OS supports RADIUS authentication, authorization, and accounting service (AAA). When configured for RADIUS, the switch becomes a Network Access Server (NAS) that acts as a RADIUS client. In this configuration, authentication records are stored in the RADIUS host server database. Login and logout account name, assigned role, and time accounting records are also stored on the RADIUS server.

You should set up RADIUS service through a secure connection, such as SSH.

Use the AAA Service tab of the Switch Admin module to manage the RADIUS server (see Figure 22).



sw48k_5_wt_91 - Switch Admin. - Microsoft Internet Explorer

SwitchName: sw48k_5_wt_91 DomainID: 1 WWN: 10:00:00:60:69:e4:00:36 Fri Mar 18 2005 16:40:54 UTC

AAA Services

Primary AAA Service: Switch Database

Secondary AAA Service: None

RADIUS Configuration

RADIUS Server	Port	Timeout(s)	Authentication
192.168.0.1	1812	3	CHAP
1.1.1.1	1812	3	CHAP
192.168.0.0	1812	3	CHAP

```
[Switch Administration opened]: Fri Mar 18 2005 13:32:09 UTC
[Switch Administration closed]: Fri Mar 18 2005 15:33:31 UTC
[Switch Administration opened]: Fri Mar 18 2005 15:34:38 UTC
```

Add RADIUS server configuration

Figure 22 AAA Service tab

Enabling and disabling RADIUS service

At least one RADIUS server must be configured before you can enable RADIUS service.

1. Launch the Switch Admin module as described on page 36.
2. Click the **AAA Service** tab.
3. To enable RADIUS service, select a RADIUS service from the Primary AAA Service drop-down list, select **None** or **Switch Database** from the Secondary AAA Service drop-down list.

   To disable RADIUS service, select **Switch Database** from the Primary AAA Service drop-down list and select **None** from the Secondary AAA Service drop-down list.
4. Click **Apply**.

Configuring the RADIUS server

The configuration is chassis-based, so it applies to all logical switches (domains) on the switch and replicates itself on a standby CP, if one is present. It is saved in a configuration upload, and so it can be applied to other switches in a configuration download. You should configure at least two RADIUS servers so that if one fails, the other assumes service.

You can configure the RADIUS server even if it is disabled. You can configure up to five RADIUS servers. You must be logged in as admin or switchAdmin to configure the RADIUS server.

To configure the RADIUS server

1. Launch the Switch Admin module as described on page 36.
2. Click the **AAA Service** tab.
3. Click **Add**.

   The RADIUS Configuration dialog box opens.

NOTE: You can configure up to five RADIUS servers. If five RADIUS servers are already configured, the Add button is disabled.

4. Enter the RADIUS server name, which is a valid IP address or Dynamic Name Server (DNS) string. Each RADIUS server must have a unique IP address or DNS name for the RADIUS server.
5. Optional: Enter the port number.
6. Optional: Enter the secret string.
7. Optional: Enter the timeout time in minutes.
8. Optional: Select an authentication protocol from CHAP or PAP.

   The default value is CHAP; if you do not change it, CHAP becomes the authentication protocol.
9. Click **OK** to return to the AAA Service tab.
10. Click **Apply**.

Modifying the RADIUS server

Use the following procedure to change the parameters of a RADIUS server that is already configured.

1. Launch the Switch Admin module as described on page 36.
2. Click the **AAA Service** tab.
3. Click a RADIUS server from the RADIUS Configuration list.
4. Click **Modify**.

   The RADIUS Configuration dialog box opens.
5. Enter new values for the port number, secret string, and timeout time (in minutes).
6. Select an authentication protocol from CHAP or PAP.

   The default value is CHAP; if you do not change it, CHAP becomes the authentication protocol.
7. Click **OK** to return to the AAA Service tab.
8. Click **Apply**.

Modifying the RADIUS server order

The RADIUS servers are contacted in the order they are listed, starting from the top of the list and moving to the bottom.

Modifying the order in which the RADIUS servers are contacted

1. Launch the Switch Admin module as described on page 36.
2. Select the **AAA Service** tab.
3. Click a RADIUS server from the RADIUS Configuration list.
4. Click the up and down arrows to rearrange the order of the RADIUS servers.
5. Click **Apply**.

Removing a RADIUS server

Use the following procedure to remove a RADIUS server.

1. Launch the Switch Admin module as described on page 36.
2. Select the **AAA Service** tab.
3. Select a RADIUS server from the RADIUS Configuration list.
4. Click **Remove**.

   If there is no RADIUS server configured, the Remove button is disabled. You cannot remove the only RADIUS server, if the RADIUS service is the primary AAA service.

   The RADIUS server is not deleted until you apply the changes from the AAA Services tab.
5. Click **Apply** in the AAA Services tab.

   A confirmation is displayed, warning you that you are about to remove the selected RADIUS server.
6. Click **Yes** in the confirmation.

6 Routing traffic

This chapter contains the following information:

Introducing routing

For Fabric OS 5.x, the supported routing policies are:

- Port-based
- Device-based (4Gb SAN Switch for HP p-Class BladeSystem and SAN Switch 4/32 only)
- Exchanged-based (4Gb SAN Switch for HP p-Class BladeSystem, SAN Switch 4/32, and 4/256 SAN Director only)

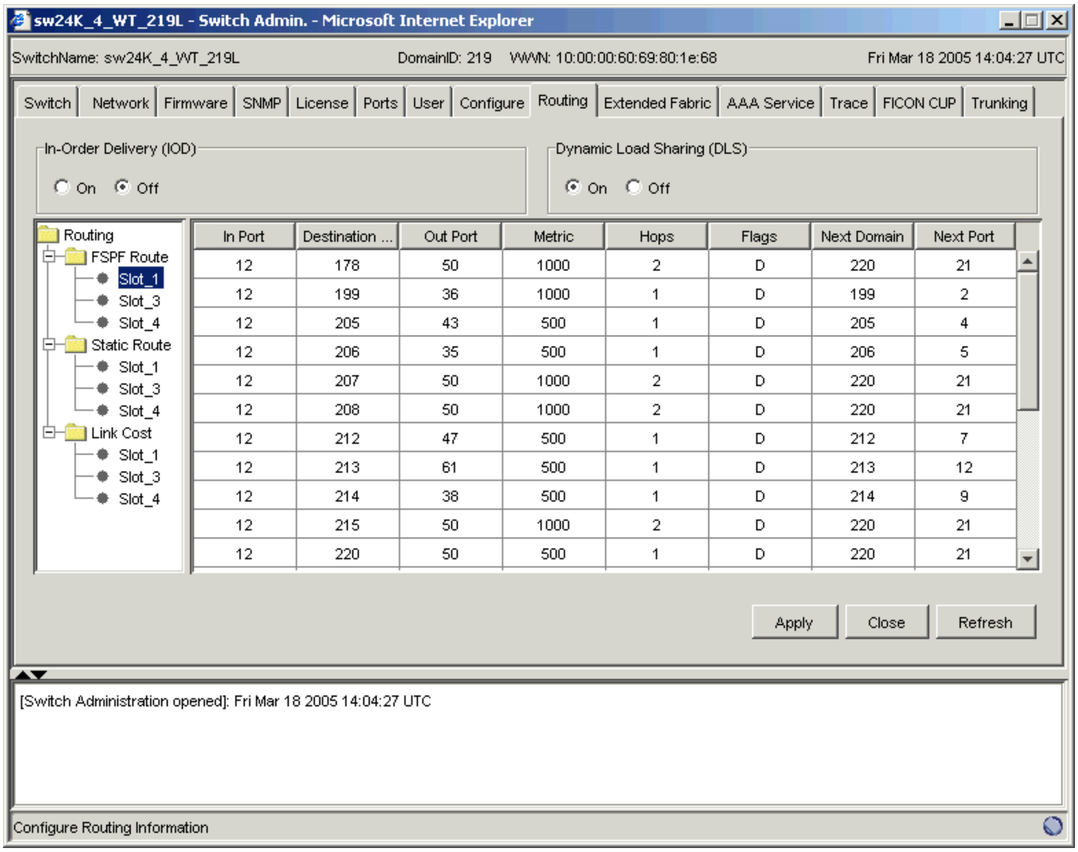
For the 4Gb SAN Switch for HP p-Class BladeSystem, SAN Switch 4/32, and 4/256 SAN Director, the exchange-based routing policy is the default.

Using port-based routing, you can assign a *static route*, in which the path chosen for traffic never changes. In contrast, device-based and exchange-based routing policies always employ *dynamic path selection*, in which the software chooses a path based on current traffic conditions. See the *HP StorageWorks Fabric OS 5.x administrator guide* for more information.

To optimize port-based routing, the dynamic load sharing (DLS) feature can be enabled to balance the load across the available output ports within a domain. Device-based and exchange-based routing require the use of DLS; when these policies are in effect, you cannot disable the DLS feature.

To configure routing policies, you must use the CLI. After the routing policies are configured, you can use Advanced Web Tools to display the routing paths, configure static routes, and configure routing parameters, such as DLS, frame order delivery, and link cost.

The Routing tab of the Switch Admin module displays routing information. Figure 23 shows the Routing tab when the port-based routing policy is enabled. When a device-based or exchange-based routing policy is enabled, the interface is different: the Static Route information and the DLS radio buttons are not displayed.



SwitchName: sw24K_4_WT_219L DomainID: 219 WWN: 10:00:00:60:69:80:1e:68 Fri Mar 18 2005 14:04:27 UTC

In-Order Delivery (IOD): ○ On ● Off

Dynamic Load Sharing (DLS): ● On ○ Off

In Port	Destination ...	Out Port	Metric	Hops	Flags	Next Domain	Next Port
12	178	50	1000	2	D	220	21
12	199	36	1000	1	D	199	2
12	205	43	500	1	D	205	4
12	206	35	500	1	D	206	5
12	207	50	1000	2	D	220	21
12	208	50	1000	2	D	220	21
12	212	47	500	1	D	212	7
12	213	61	500	1	D	213	12
12	214	38	500	1	D	214	9
12	215	50	1000	2	D	220	21
12	220	50	500	1	D	220	21

[Switch Administration opened]: Fri Mar 18 2005 14:04:27 UTC

Configure Routing Information

Figure 23 Routing tab for port-based routing policy

Displaying FSPF routing

The Routing tab of the Switch Admin module displays information about routing paths.

Viewing FSPF routing

1. Launch the Switch Admin module as described on page 36.
2. Click the **Routing** tab.
3. Perform the following, according to switch type:
   - For Core Switch 2/64, SAN Director 2/128, or 4/256 SAN Director, click a slot number under the FSPF Route category in the navigation tree.
   - For 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, 4Gb SAN Switch for HP p-Class BladeSystem, and SAN Switch 4/32, click the FSPF Route category in the navigation tree.

Configuring a static route

A static route can be assigned only when the active routing policy is port-based. When device-based or exchange-based routing is active, you cannot disable DLS and you cannot view and configure static routes.

When you configure a static route for a Core Switch 2/64 or for a SAN Director 2/128 or 4/256 SAN Director configured for two logical switches, the static route is configured on a logical-switch basis. This means that for each logical switch, you must configure a static route individually.

To configure a static route

1. Launch the Switch Admin module as described on page 36.
2. Click the **Routing** tab.

3. Perform the following, according to switch type:
   - For Core Switch 2/64, SAN Director 2/128, or 4/256 SAN Director, click a slot number under the Static Route category in the navigation tree. Click **Add**.
   - For 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, 4Gb SAN Switch for HP p-Class BladeSystem, and SAN Switch 4/32, click the Static Route category in the navigation tree. Click **Add**.

   A new blank line appears in the window. Note that when device-based or exchange-based routing policies are in effect, the Static Route category is not displayed in the navigation tree.
4. Enter the In Port number for the route.
5. Enter the Destination Domain.

   The destination domain IDs match the outports in the cell.
6. Enter the Out Port number for the route.
7. Click **OK** to add the static route.
8. Click **Apply**.

Enabling and disabling dynamic load sharing

The device-based and exchange-based routing policies depend on the Fabric OS DLS for dynamic routing path selection. When these policies are in force, DLS is always enabled and cannot be disabled.

When the port-based policy is in force, you can enable DLS to optimize routing. When DLS is enabled, it shares traffic among multiple equivalent paths between switches. DLS recomputes load sharing either when a switch boots up or each time an E_Port or Fx_Port goes online or offline. Enabling this feature allows a path to be discovered by the FSPF path-selection protocol.

For more information regarding DLS, see the `dlsset` command in the *HP StorageWorks Fabric OS 5.x command reference guide*.

When you enable or disable DLS for the Core Switch 2/64 or for a SAN Director 2/128 or 4/256 SAN Director configured for two logical switches, the DLS is enabled or disabled on a logical-switch basis. This means that for each logical switch, you must enable or disable DLS individually.

Configuring the DLS setting

1. Launch the Switch Admin module as described on page 36.
2. Select the **Routing** tab.
3. Click **On** in the Dynamic Load Sharing area to enable DLS or click **Off** to disable DLS.

   Note that when device-based or exchange-based routing policies are in effect, the DLS radio buttons are not displayed in the Routing tab.
4. Click **Apply**.

Specifying frame order delivery

In a stable fabric, frames are always delivered in order, even when the traffic between switches is shared among multiple paths. However, when topology changes occur in the fabric (for example, if a link goes down), traffic is rerouted around the failure, and some frames could be delivered out of order.

By default, frame delivery is out-of-order across topology changes. However, if the fabric contains destination devices that do not support out-of-order delivery, you can force in-order frame delivery across topology changes.

Enabling in-order delivery (IOD) guarantees that frames are either delivered in order or dropped. For more information regarding IOD, see the *HP StorageWorks Fabric OS 5.x administrator guide*.

When you enable or disable IOD for the Core Switch 2/64 or for a SAN Director 2/128 or 4/256 SAN Director configured for two logical switches, IOD is enabled or disabled on a logical-switch basis. This means that for each logical switch, you enable or disable IOD individually.

NOTE: Enabling IOD can cause a delay in the establishment of a new path when a topology change occurs, and therefore should be used with care.

Configuring the IOD setting

1. Launch the Switch Admin module as described on page 36.
2. Click the **Routing** tab.
3. Click **On** in the In-Order Delivery area to force in-order frame delivery across topology changes or click **Off** to restore out-of-order frame delivery across topology changes.
4. Click **Apply**.

Configuring link cost

When you configure link cost for the Core Switch 2/64, or for a SAN Director 2/128, or 4/256 SAN Director configured for two logical switches, link cost is configured on a logical-switch basis. This means that for each logical switch, you configure link cost individually.

For information regarding link cost, see the `linkCost` command in the *HP StorageWorks Fabric OS 5.x command reference guide*.

Configuring the link cost for a port

1. Launch the Switch Admin module as described on page 36.
2. Click the **Routing** tab.
3. Perform the following, according to switch type:
   - For Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, click the slot number of the logical switch under Link Cost in the navigation tree.
   - For 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, 4Gb SAN Switch for HP p-Class BladeSystem, and SAN Switch 4/32, click Link Cost in the navigation tree.
4. Double-click in the row in the Cost column that corresponds to the appropriate port.
5. Enter the link cost. For a 1 Gbit/sec ISL, the default cost is 1000.

   For a 2 Gbit/sec or a 4 Gbit/sec ISL, the default cost is 500. Valid values for link cost are 1 through 9999. Setting the value to 0 sets the link cost to the default value for that port.
6. Click **Apply**.

7 Administering extended fabrics

This chapter contains the following information:

About extended link buffer allocation

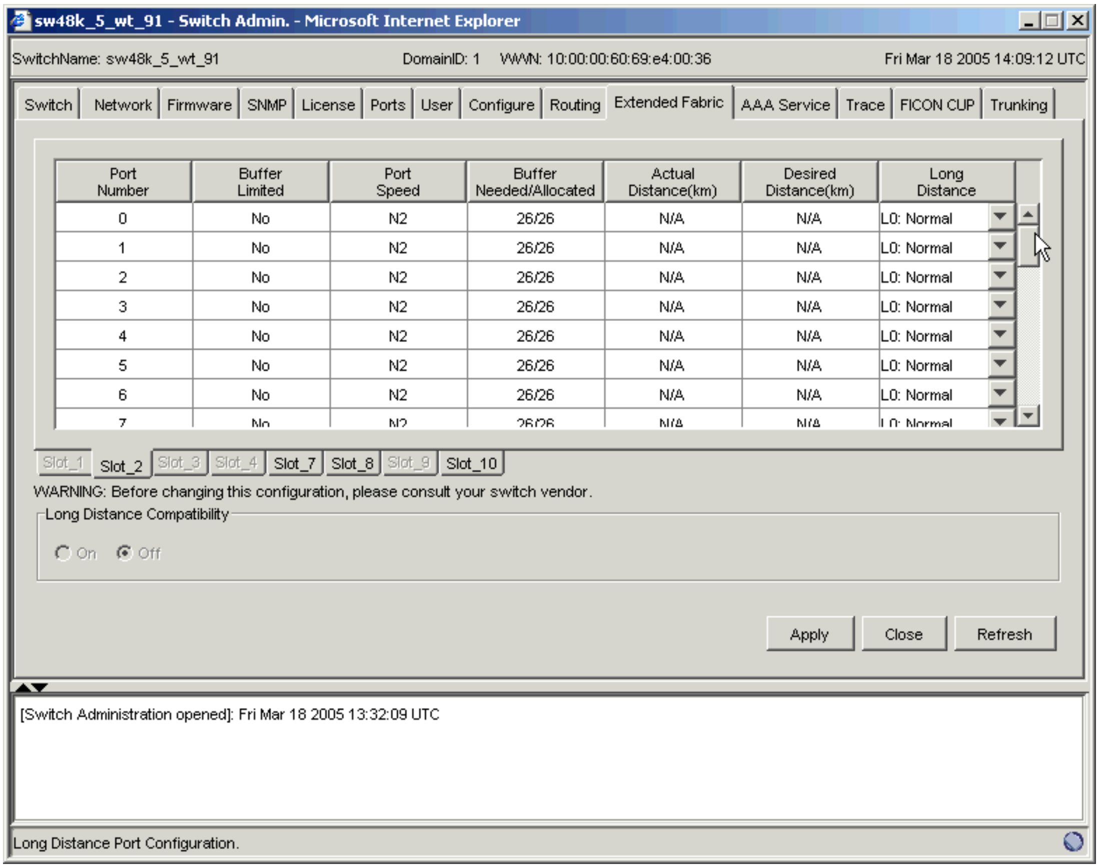
As the distance between switches and the link speed increases, additional buffer-to-buffer credits are required to maintain maximum performance. The number of credits reserved for a port depends on the switch model and on the extended ISL mode for which it is configured.

The Extended Fabric tab of the Switch Admin module displays information about the port speed, long-distance setting, and buffer credits, as shown in Figure 24. Use this tab to configure the long-distance setting of a port. For detailed information on managing extended fabrics, see the *HP StorageWorks Fabric OS 5.x administrator guide*.

The Extended Fabric tab provides the following information:

- Port Number
- Buffer Limited: A buffer-limited port can come online with fewer buffer credits allocated than its configuration specifies, allowing it to operate at a reduced bandwidth instead of being disabled for lack of buffers.

  Buffer-limited operation is supported for the L0 and LD extended ISL modes only and is persistent across reboots, switch disabling and enabling, and port disabling and enabling.
- Port Speed, which is displayed as follows:
  - 1G 1 Gbit/sec
  - 2G 2 Gbit/sec
  - 4G 4 Gbit/sec
  - N1 Negotiated 1 Gbit/sec
  - N2 Negotiated 2 Gbit/sec
  - N4Negotiated 4 Gbit/sec
  - Auto-Negotiation
- Buffer Needed/Allocated: The number of buffers needed and the number of buffers that are actually allocated.
- Actual Distance: The actual distance, in kilometers, for the link.
- Desired Distance: Required for a port configured in LD mode (see Table 9), the desired distance, in kilometers, for the link. This value is the upper limit for calculating buffer availability for the port. If the measured distance is more than the specified desired distance, the port is allocated the number of buffers required by the specified desired distance.
- Long Distance: Table 9 describes the long-distance settings and identifies which settings require an Extended Fabrics license.



SwitchName: sw48k_5_wt_91 DomainID: 1 WWN: 10:00:00:60:69:e4:00:36 Fri Mar 18 2005 14:09:12 UTC

Port Number	Buffer Limited	Port Speed	Buffer Needed/Allocated	Actual Distance(km)	Desired Distance(km)	Long Distance
0	No	N2	26/26	N/A	N/A	L0: Normal
1	No	N2	26/26	N/A	N/A	L0: Normal
2	No	N2	26/26	N/A	N/A	L0: Normal
3	No	N2	26/26	N/A	N/A	L0: Normal
4	No	N2	26/26	N/A	N/A	L0: Normal
5	No	N2	26/26	N/A	N/A	L0: Normal
6	No	N2	26/26	N/A	N/A	L0: Normal
7	No	N2	26/26	N/A	N/A	L0: Normal

WARNING: Before changing this configuration, please consult your switch vendor.

Long Distance Compatibility

○ On ● Off

[Switch Administration opened]: Fri Mar 18 2005 13:32:09 UTC

Long Distance Port Configuration.

Figure 24 Extended Fabric tab

Table 9 Long-distance settings and license requirements

Value	Description	Extended fabric license required?
L0	No long-distance setting is enabled. The maximum supported link distance is 10 km, 5 km, or 2.5 km for ports at speeds of 1 Gbit/sec, 2 Gbit/sec, and 4 Gbit/sec, respectively.	No
LE	Extended normal setting is enabled, 10 km (6 miles) or less.	No
L0.5	Setting of 25 km (15.5 miles) or less is enabled.	Yes
L1	Medium long-distance setting is enabled, 50 km (31 miles) or less.	Yes
L2	Long-distance setting is enabled, 100 km (62 miles) or less.	Yes
LD	Dynamic setting is enabled. The LD-level link can operate at distances up to 500 km at 1 Gbit/sec, 250 km at 2 Gbit/sec, or 125 km at 4 Gbit/sec, depending on the availability of frame buffers within the port group.	Yes

Configuring for long distance

When you configure a long-distance ISL, ensure that the ports on both sides of the ISL have the same configuration, to avoid fabric segmentation.

Configuring a port for long-distance connection

1. Launch the Switch Admin module as described on page 36.
2. Click the **Extended Fabric** tab.

3. Perform the following, according to switch type:
   - For Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, click the slot subtab that corresponds to the correct slot for the logical switch.
   - For 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, 4Gb SAN Switch for HP p-Class BladeSystem, and SAN Switch 4/32, proceed directly to the next step.
4. Select a port by clicking anywhere in the row for that port.
5. Select a distance from the Long Distance drop-down list that corresponds to the port.

   Depending on the distance selected, this might require an optional license. For information about the various distances, see Table 9.

   If you select a long-distance setting of LD, you must also enter a value in the Desired Distance column for that port number:

   a. Double-click the **Desired Distance** box for the port, as shown in Figure 24 on page 76.
   b. Enter a number in the field to indicate the distance in kilometers:
      - For 1 Gbit/sec ports, enter a number between 10 and 500, inclusive.
      - For 2 Gbit/sec ports, enter a number between 10 and 250, inclusive.
      - For 4 Gbit/sec ports, enter a number between 10 and 125, inclusive.

      This value is the upper limit for calculating buffer availability for other ports in the same port group. If the actual distance is more than the desired distance, the port operates in buffer-limited mode.
   c. Press **Enter** or click another port entry for the value to be accepted.
6. Optional: If the fabric contains HP StorageWorks 1 GB switches extended ISLs, select the **On** radio button for Long Distance Compatibility. The switch must be disabled before you can select this option.

   If you select this option, you must have an Extended Fabrics license, and both E_Ports in an ISL must be configured with the same long-distance compatibility setting. The SAN Switch 4/32 cannot be part of such a fabric.
7. Click **Apply**.

8 Administering ISL trunking

This chapter contains the following information:

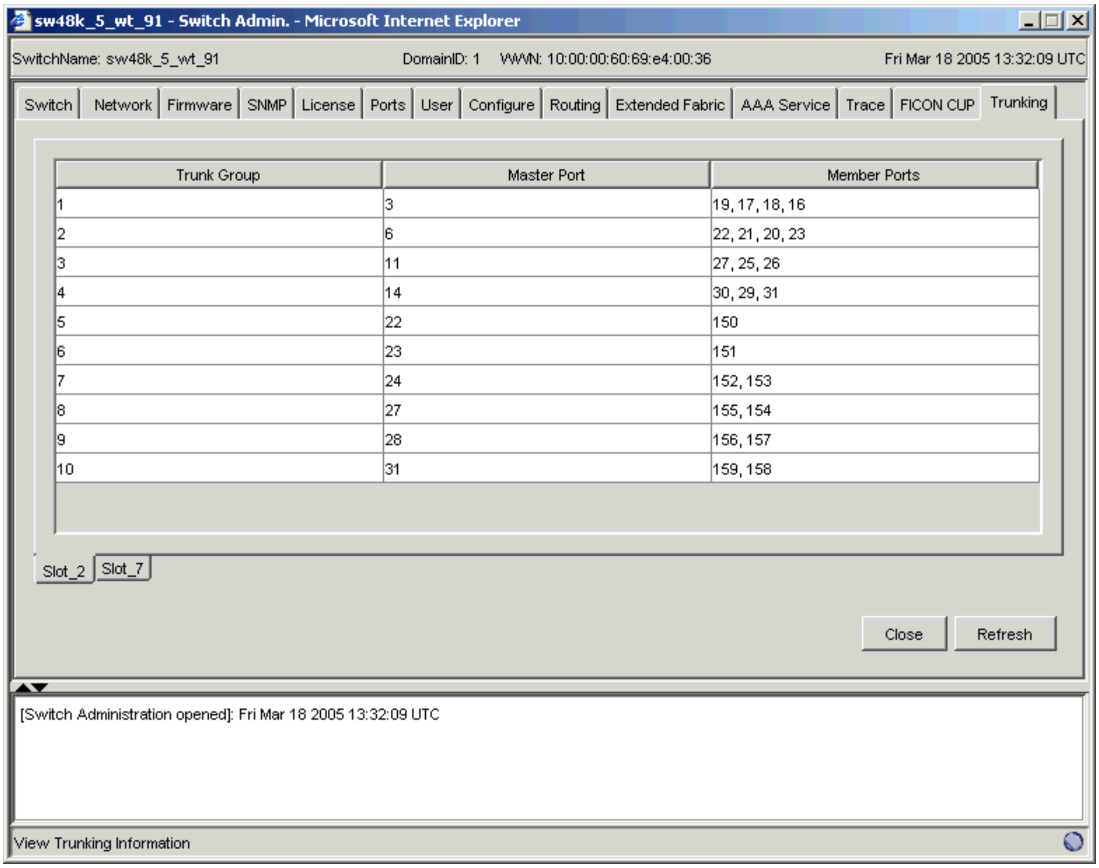
- Displaying trunk group information, page 79
- Disabling or reenabling trunking mode on a port, page 80

ISL trunking optimizes network performance by forming trunking groups that can distribute traffic across a shared bandwidth.

A trunking license is required on each switch that participates in the trunk. (For details on obtaining and installing licensed features, see "Maintaining licensed features" on page 47.)

For additional information about ISL Trunking, see the *HP StorageWorks Fabric OS 5.x administrator guide*.

Use the Trunking tab of the Switch Admin module to view and manage trunks through Advanced Web Tools (see Figure 25).



SwitchName: sw48k_5_wt_91 DomainID: 1 WWN: 10:00:00:60:69:e4:00:36 Fri Mar 18 2005 13:32:09 UTC

Trunk Group	Master Port	Member Ports
1	3	19, 17, 18, 16
2	6	22, 21, 20, 23
3	11	27, 25, 26
4	14	30, 29, 31
5	22	150
6	23	151
7	24	152, 153
8	27	155, 154
9	28	156, 157
10	31	159, 158

[Switch Administration opened]: Fri Mar 18 2005 13:32:09 UTC

Figure 25 Trunking tab

Displaying trunk group information

Use this procedure to display the following information about ISL Trunking groups:

- Trunk group number identifier
- Master port
- Member ports

Viewing information on a trunk group

1. Launch the Switch Admin module as described on page 36.
2. Select the **Trunking** tab.
3. Optional: Click **Refresh** to refresh the information.

Disabling or reenabling trunking mode on a port

When the trunking license is activated, trunks are established on eligible ISLs and trunking capability is enabled by default on all ports. Use the following procedure to disable trunking on a port or to reenable trunking if it has been disabled.

1. Launch the Switch Admin module as described on page 36.
2. Select the **Ports** tab (see Figure 10 on page 44).
3. Perform the following, according to switch type:
   - For Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, click the slot subtab that corresponds to the correct slot for the logical switch.
   - For 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, 4Gb SAN Switch for HP p-Class BladeSystem, and SAN Switch 4/32, proceed directly to the next step.
4. To enable trunking mode on a port, select the check box in the Enable Trunking column that corresponds to the port you want to trunk.

   To disable trunking mode on a port, clear the box.
5. Click **Apply**.

9 Administering zoning

This chapter briefly describes zoning and provides the procedures for managing zoning using Advanced Web Tools. It contains the following sections:

Introducing zoning

Zoning enables you to partition your SAN into logical groups of devices that can access each other. For example, you can partition your SAN into two zones, *winzone* and *unixzone*, so that your Windows servers and storage do not interact with your UNIX® servers and storage.

Zones can be configured dynamically. They can vary in size, depending on the number of fabric-connected devices, and devices can belong to more than one zone. Because zone members can access only other members of the same zone, a device not included in a zone is not available to members of that zone.

When using a mixed fabric—that is, a fabric containing 5.x, 4.x, 3.x, and 2.x switches—you should use the switch with the highest Fabric OS level to perform zoning tasks. See "Entering a zone alias in the Define Device Alias wizard" on page 102 for more recommendations about zoning.

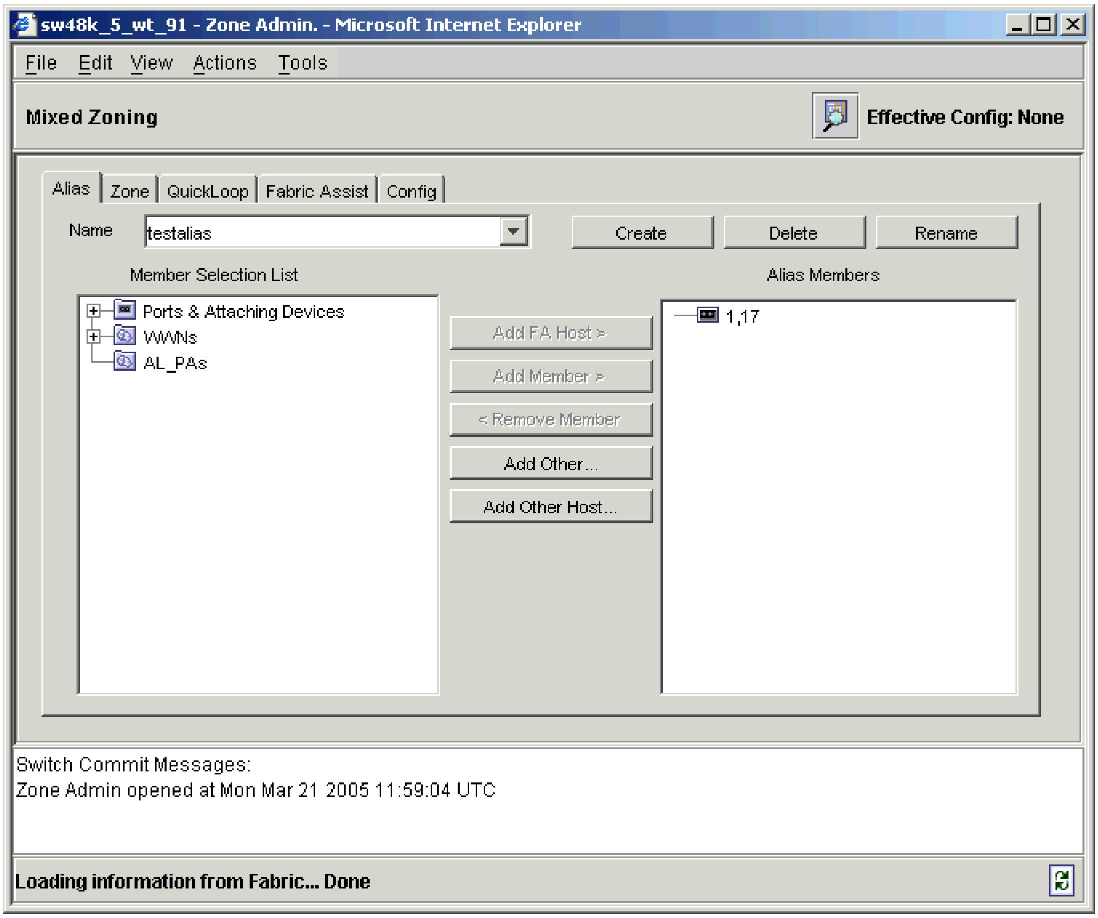
When zone or Fabric Assist (FA) zone members are specified by fabric location (domain, area) only, or by device name (node name or port WWN) only, then zone boundaries can be enforced at the hardware level, and the zone is referred to as a *hard zone*.

When zone elements are specified by fabric location (domain, area) and other elements of the same zone are specified by device name (node name or port WWN), zone enforcement depends on Name Server lookups, and the zone is referred to as a *soft zone*.

For more specific information about zoning concepts, see the *HP StorageWorks Fabric OS 5.x administrator guide*.

Managing zoning with Advanced Web Tools

You can monitor and manage zoning through the Advanced Web Tools Zone Admin module. Click the **Zone Administration** icon in the Fabric Toolbar to access the Zone Admin module, shown in Figure 26. The Zone Admin icon is displayed in the Fabric Toolbar only if an Advanced Zoning license is installed on the switch.



Mixed Zoning

Effective Config: None

Name testalias

Switch Commit Messages:
Zone Admin opened at Mon Mar 21 2005 11:59:04 UTC

Loading information from Fabric... Done

Figure 26 Zone Admin Module

The information in the Zone Admin module is collected from the selected switch.

If secure mode is enabled, zoning can be administered only from the primary FCS switch. If the selected switch has an Advanced Zoning license installed but is not the primary FCS switch, the Zone Admin icon is displayed in the Fabric Toolbar but not activated. For specific information regarding secure fabrics, see the *HP StorageWorks Secure Fabric OS administrator guide*.

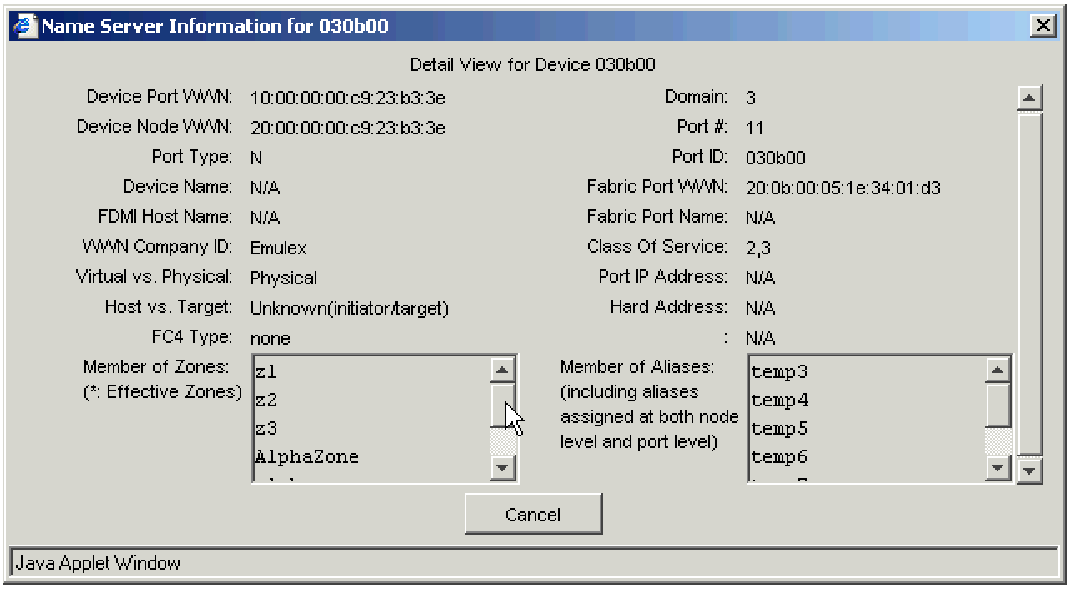
You must be logged in as an admin or switchAdmin to launch the Zone Admin module. If you are logged in as a switchAdmin, you can access the Zone Admin module in read-only mode only; most of the zoning operations are disabled in read-only mode.

A snapshot is taken of all the zoning configurations at the time you launch the Zone Admin module; this information is not updated by Advanced Web Tools. To update this information, see "Refreshing the Zone Admin module information" on page 84.

NOTE: Any changes you make in the Zone Admin module are held in a buffered environment and do not update the zoning database until you save the changes. If you close the Zone Admin module without saving your changes, your changes are lost. To save the buffered changes you make in the Zone Admin module to the zoning database on the switch, see "Saving local zoning changes" on page 84.

Saving means updating the zoning database on the switch with the local changes from the Advanced Web Tools buffer. *Refreshing* means copying the current state of the zoning database on the switch to the Advanced Web Tools buffer, overwriting its current contents.

In the Zone Admin module, all WWNs also display vendor names. In the Member Selection List panel (see Figure 27), you can right-click port and device nodes to display which aliases the port or device is a member of. In addition, you can right-click the device nodes and then select View Device Detail to display detailed information about the selected device, as shown in Figure 27.



Detail View for Device 030b00

Device Port WWN:	10:00:00:00:c9:23:b3:3e	Domain:	3
Device Node WWN:	20:00:00:00:c9:23:b3:3e	Port #:	11
Port Type:	N	Port ID:	030b00
Device Name:	N/A	Fabric Port WWN:	20:0b:00:05:1e:34:01:d3
FDMI Host Name:	N/A	Fabric Port Name:	N/A
WWN Company ID:	Emulex	Class Of Service:	2,3
Virtual vs. Physical:	Physical	Port IP Address:	N/A
Host vs. Target:	Unknown(initiator/target)	Hard Address:	N/A
FC4 Type:	none	:	N/A
Member of Zones: (*: Effective Zones)	z1 z2 z3 AlphaZone	Member of Aliases: (including aliases assigned at both node level and port level)	temp3 temp4 temp5 temp6

Figure 27 Device detail example

NOTE: In the Detail View window, the scroll bars in the **Member of Zones** and **Member of Aliases** sections do not scroll unless you double-click them first.

The remainder of this section describes basic zoning procedures you can perform in the Zone Admin module that are useful for all zoning operations.

Launching the Zone Admin module

This section describes how to launch the Zone Admin module, from which all zoning procedures are performed.

1. Select a switch from the Fabric Tree.

   The selected switch appears in the Switch View.

2. Click the **Zone Administration** icon in the Fabric Toolbar.

   The Zone Admin module is displayed (see Figure 26 on page 82).

Refreshing the fabric information

This function refreshes the display of fabric elements (switches, ports, devices, and AL_PAs) only. It does not affect any zoning element changes or update zone information in the Zone Admin module. To refresh the zone information displayed in the Zone Admin module, see "Refreshing the Zone Admin module information" next.

This option allows you to refresh the fabric element information displayed at any time.

To refresh the fabric information

In the Zone Admin module, select **View > Refresh Fabric**.

This refreshes the status for the fabric, including switches, ports, and devices.

Refreshing the Zone Admin module information

The information displayed in the Zone Admin module is initially a snapshot of the contents of the fabric zoning database at the time the module is launched. Any changes you make to this window are saved to a local buffer; they are not applied to the fabric zoning database until you invoke one of the transactional operations listed in the Actions menu.

Any local zoning changes are buffered by the Zone Admin module until explicitly saved to the fabric. If the fabric zoning database is independently changed by another user or from another interface (for example, the CLI) while Advanced Web Tools zoning changes are still pending, the refresh icon starts to blink (after a 15 second polling delay). You can then choose to refresh the current Advanced Web Tools zoning view to reflect the new, externally changed contents of the fabric zoning database, in which case any pending local changes are lost, or you can ignore the blinking refresh icon and save your local changes, overwriting the external changes that triggered the icon to blink.

Another reason to refresh zoning is to back out of current, unsaved work and start over.

You can refresh the zoning information at any time, either using the refresh icon (whether it is flashing or not) or from the View menu.

The following procedure updates the information in the Zone Admin module with the information saved in the zoning database on the switch.

△ **CAUTION:** When you refresh the buffered information in the Zone Admin module, any zoning configuration changes you have made and not yet saved are erased from the buffer and replaced with the currently enabled zone configuration information that is saved on the switch.

Refreshing the local Zone Admin buffer from the fabric zoning database

1. Launch the Zone Admin module as described on page 83.
2. Select **View > Refresh Zoning** or click the zone refresh icon (located in the lower right corner of the Zone Admin module).

   This refreshes the information in the Zone Admin module with the information in the switch's zoning database. This action also refreshes the fabric information as described in "Refreshing the fabric information" on page 83. Any unsaved zoning changes are deleted.

Saving local zoning changes

All information displayed and all changes made in the Zone Admin module are buffered until you save the changes. That means that any other user looking at the zone information for the switch does not see the changes you have made until you save them.

Saving the changes propagates any changes you have made in the Zone Admin module (buffered changes) to the zoning database on the switch. If another user has a zoning operation in progress at the time that you attempt to save changes, a warning is displayed that indicates that another zoning transaction is in progress on the fabric. You can select to abort the other transaction and override it with yours.

If the zoning database size exceeds the maximum allowed, you cannot save the changes. The zoning database summary displays the maximum zoning database size (see "Displaying the zone configuration summary" on page 96).

This action updates the entire contents of the Zone Admin module, not just the selected zone, alias, or configuration. You can save your changes at any time during the zone administration session.

Saving Zone Admin module changes to the switch zoning database

1. Make your zoning changes in the Zone Admin module.
2. Select **Actions > Save Config Only**.

NOTE: If you made changes to a configuration, you must enable the configuration before the changes become effective. To enable the configuration, see "Enabling a zone configuration" on page 94.

Closing the Zone Admin module

It is very important to remember that any changes you make in the Zone Admin module are not saved. It is recommended that you always close the Zone Admin module from the File menu, as described in the procedure below.

△ **CAUTION:** If you click the X in the top right corner of the Zone Admin module, the Zone Admin session is closed immediately, and any changes you made without saving are lost. To avoid potential loss of data, use the following procedure to close the Zone Admin module. In this procedure, the Zone Admin session displays a warning if you have unsaved changes when you are trying to close the Zone Admin module.

Safely closing the Zone Admin module

1. From the Zone Admin module, select **File > Close**.

   If any changes exist in the buffer that have not been saved, a warning dialog box opens, asking you to confirm that you want to close the Zone Admin session without saving the changes.
2. Click **Yes** to close without saving changes, or click **No** to go back to the Zone Admin module to save the changes as described in "Saving local zoning changes" on page 84.

Zoning views

You can choose how zoning elements are displayed in the Zone Admin module. The zoning view you select determines how members are displayed in the Member Selection List panel (see Figure 26 on page 82). The views filter the fabric and device information displayed in the Member Selection List for the selected view, making it easier for you to create and modify zones, especially when creating hard zones.

Depending on the method you use to zone, certain tabs might or might not be available in the Zone Admin window.

There are four views of defining members for zoning:

- Mixed zoning, which displays the port area number, device WWNs, or QuickLoop AL_PAs, and is useful when creating a soft zone
- Port zoning, which displays port area numbers only, and is useful when creating a hard zone
- WWN zoning, which displays device WWNs only, and is useful when creating a hard zone
- AL_PA zoning, which displays QuickLoop AL_PAs only, and is useful when creating a soft zone

Selecting a zoning view

1. Launch the Zone Admin module as described on page 83.
2. From the View menu, select one of the following:
   - Mixed Zoning
   - Port Zoning
   - WWN Zoning
   - AL_PA Zoning

Managing zone aliases

An alias is a logical group of port area numbers, WWNs, or AL_PAs. Specifying groups of ports or devices as an alias makes zone configuration easier, by enabling you to configure zones using an alias rather than inputting a long string of individual members. You can specify members of an alias using the following methods:

- A switch domain and port area number pair: for example, `2, 20`
- Device node and device port WWNs
- QuickLoop AL_PAs

Creating and populating a zone alias

Use the following procedure to create a zone alias.

Creating an alias

1. Launch the Zone Admin module as described on page 83.
2. Select a format to display zoning members in the Member Selection List as described in "Zoning views" on page 85.
3. Click the **Alias** tab.
4. Click **Create**.

   The Create New Alias dialog box opens.
5. Enter a name for the new alias, and click **OK** in the Create New Alias dialog box.

   The new alias is displayed in the Name list in the Alias tab.
6. Click **+** signs in the Member Selection List to view the nested elements.

   The choices available in the Member Selection List depend on the selection made in the View menu.
7. Select elements in the Member Selection List that you want to include in your alias.

   The Add Member button becomes active.
8. Click **Add Member** to add alias members.

   Selected members move to the Alias Members window.
9. Optional: Repeat step 7 and step 8 to add more elements to your alias.
10. Optional: Click **Add Other** to include a WWN, port, or QuickLoop (AL_PA) that is not currently a part of the fabric.
11. Optional: Click **Add Other Host** to include a WWN, port, or QuickLoop (AL_PA) that is not currently a part of the fabric.

Adding and removing members of a zone alias

Use the following procedure to add or remove zone alias members.

Modifying the members of an alias

1. Launch the Zone Admin module as described on page 83.
2. Click the **Alias** tab.
3. Select the alias you want to modify from the Name drop-down list.
4. Highlight an element in the Member Selection List that you want to add to your alias, or highlight an element in the Alias Members list that you want to delete.
5. Click **Add Member** to add the selected alias member, or click **Remove Member** to remove the selected alias member.

   The alias is modified in the Zone Admin buffer.

Renaming a zone alias

Use the following procedure to change the name of a zone alias.

1. Launch the Zone Admin module as described on page 83.
2. Click the **Alias** tab.
3. Select the alias you want to rename from the Name drop-down list.
4. Click **Rename**.

   The Rename an Alias dialog box opens.
5. Enter a new alias name and click **OK**.

   The alias is renamed in the Zone Admin buffer.

Deleting a zone alias

You can remove a zone alias from the Zone Admin buffer. When a zone alias is deleted, it is no longer a member of the zones of which it was once a member.

1. Launch the Zone Admin module as described on page 83.
2. Click the **Alias** tab.
3. Select the alias you want to delete from the Name drop-down list.
4. Click **Delete**.

   The Confirm Deleting Alias dialog box opens.
5. Click **Yes**.

   The selected alias is deleted from the Zone Admin buffer.

Managing zones

A zone is a region within the fabric in which specified switches and devices can communicate. A device can communicate only with other devices connected to the fabric within its specified zone. You can specify members of a zone using the following methods:

- Alias names
- Switch domain and port area number pair: for example, `2, 20`.
- WWN (device)
- QuickLoop AL_PAs (device)

Creating and populating a zone

Use the following procedure to create a zone.

Creating a zone

1. Launch the Zone Admin module as described on page 83.
2. Select a format to display zoning members in the Member Selection List as described in "Zoning views" on page 85.
3. Click the **Zone** tab.
4. Click **Create**.

   The Create New Zone dialog box opens.
5. Enter a name for the new zone in the Create New Zone dialog box, and click **OK**.

   The new zone is displayed in the Name list.
6. Click **+** signs in the Member Selection List to view the nested elements.

   The choices available in the Member Selection List depend on the selection made in the View menu.
7. Select an element in the Member Selection List that you want to include in your zone.

   The Add Member button becomes active.
8. Click **Add Member** to add the zone member.

   The selected member is moved to the Zone Members window.

9. Optional: Repeat step 7 and step 8 to add more elements to your zone.
10. Optional: Click **Add Other** to include a WWN, port, or QuickLoop (AL_PA) that is not currently a part of the fabric.

Adding and removing the members of a zone

Use the following procedure to add or remove zone members.

Modifying the members of a zone

1. Launch the Zone Admin module as described on page 83.
2. Click the **Zone** tab.
3. Select the zone you want to modify from the Name drop-down list.

   The zone members for the selected zone are listed in the Zone Members list.
4. Highlight an element in the Member Selection List that you want to include in your zone, or highlight an element in the Zone Members list that you want to delete.
5. Click **Add Member** to add a zone member or click **Remove Member** to remove a zone member.

   The zone is modified in the Zone Admin buffer.

Renaming a zone

Use the following procedure to change the name of a zone.

1. Launch the Zone Admin module as described on page 83.
2. Click the **Zone** tab.
3. Select the zone you want to rename from the Name drop-down list.
4. Click **Rename**.

   The Rename a Zone dialog box opens.
5. Enter a new zone name and click **OK**.

   The zone is renamed in the Zone Admin buffer.

Deleting a zone

Use the following procedure to delete a zone.

1. Launch the Zone Admin module as described on page 83.
2. Click the **Zone** tab.
3. Select the zone you want to delete from the Name drop-down list.
4. Click **Delete**.

   The Confirm Deleting Zone dialog box opens.
5. Click **Yes**.

   The selected zone is deleted from the Zone Admin buffer.

Managing QuickLoops

QuickLoop is an HP software product that allows multiple ports on a switch to create a logical loop. Devices connected via QuickLoop appear to each other as if they are on the same arbitrated loop.

QuickLoop can be administered using Fabric OS 5.x; the following switches and directors running Fabric OS 5.x, however, cannot be members of a QuickLoop:

- Core Switch 2/64
- SAN Director 2/128
- 4/256 SAN Director
- 4/8 SAN Switch
- 4/16 SAN Switch
- SAN Switch 2/8V
- SAN Switch 2/16V

- SAN Switch 2/32
- 4Gb SAN Switch for HP p-Class BladeSystem
- SAN Switch 4/32

NOTE: You must have a QuickLoop license installed to create or modify a QuickLoop.

Creating a QuickLoop

Use the following procedure to create a QuickLoop.

1. Launch the Zone Admin module as described on page 83.
2. Select a format to display zoning members in the Member Selection List as described in "Zoning views" on page 85.
3. Click the **QuickLoop** tab.
4. Click **Create**.

   The Create New QuickLoop dialog box opens.
5. Enter a name for the new QuickLoop.
6. Click **OK**.
7. Click an element in the Member Selection List that you want to include in your QuickLoop.

   The Add Member button becomes active.

NOTE: There is a limit of two members per QuickLoop. Only switches capable of running QuickLoop are displayed in the Member Selection List.

8. Click **Add Member** to add QuickLoop members.

   Selected members are moved to the QuickLoop Members area.
9. Optional: Repeat step 7 and step 8 to add a second element to your QuickLoop.

Adding and removing members of a QuickLoop

Use the following procedure to add or remove members of a QuickLoop.

Modifying the members of a QuickLoop

1. Launch the Zone Administration module as described on page 83.
2. Click the **QuickLoop** tab.
3. Select the QuickLoop you want to modify from the Name drop-down list.
4. Highlight an element in the Member Selection List that you want to include in your QuickLoop, or highlight an element in the QuickLoop Members that you want to delete.

NOTE: There is a limit of two members per QuickLoop. Only switches capable of running QuickLoop are displayed in the Member Selection List.

5. Click **Add Member** to add a QuickLoop member or click **Remove Member** to remove a QuickLoop member.

Renaming a QuickLoop

Use the following procedure to change the name of a QuickLoop.

1. Launch the Zone Admin module as described on page 83.
2. Click the **QuickLoop** tab.
3. Select the QuickLoop you want to rename from the Name drop-down list.

4. Click **Rename**.

   The Rename a QuickLoop dialog box opens.
5. Enter a new QuickLoop name and click **OK**.

   The QuickLoop is renamed in the Zone Admin buffer.

Deleting a QuickLoop

Use the following procedure to delete a QuickLoop.

1. Launch the Zone Admin module as described on page 83.
2. Click the **QuickLoop** tab.
3. Select the QuickLoop you want to delete from the Name drop-down list.
4. Click **Delete**.

   The Confirm Deleting QuickLoop dialog box opens.
5. Click **Yes**.

   The selected QuickLoop is deleted from the Zone Admin buffer.

Managing Fabric Assist zones

FA is an extension to QuickLoop. An FA zone allows private hosts to communicate with public or private targets across the fabric.

FA zones can be administered using Fabric OS 5.x; however, the following switches and directors running Fabric OS 5.x cannot be members of an FA zone:

- Core Switch 2/64
- SAN Director 2/128
- 4/256 SAN Director
- 4/8 SAN Switch
- 4/16 SAN Switch
- SAN Switch 2/8V
- SAN Switch 2/16V
- SAN Switch 2/32
- 4Gb SAN Switch for HP p-Class BladeSystem
- SAN Switch 4/32

NOTE: You must have a QuickLoop license installed to create or modify an FA zone.

Creating a Fabric Assist zone

Use the following procedure to create an FA zone. For this example, the Mixed Zone level is used.

1. Launch the Zone Admin module as described on page 83.
2. Select **View > Mixed Zoning** (you can select any view except the AL_PA view).

   The **Mixed View** tab is displayed.
3. Click the **Fabric Assist** tab.
4. Click **Create**.

   The Create New FA dialog box opens.
5. Enter a name for the new FA zone and click **OK**.

   A fabric host is required.
6. Click **+** signs in the Member Selection List to view the nested elements.

   The choices available in the Member Selection List depend on the selection made in the View menu.

7. Select an element in the Member Selection List that you want to include in your zone.

   The Add Member button becomes active.

8. Click **Add Member** to add the zone member.

   The selected member is moved to the Zone Members window.

9. Optional: Repeat step 7 and step 8 to add more elements to your FA zone.

10. Optional: Click **Add Other** to include a WWN, port, or QuickLoop (AL_PA) that is not currently a part of the fabric.

11. Optional: Click **Add Other Host** to include a WWN, port, or QuickLoop (AL_PA) that is not currently a part of the fabric.

    The new members appear in the Fabric Assist Members area. The newly created FA zone also is displayed in the Config tab.

Adding and removing Fabric Assist zone members

Use the following procedure to add and remove FA zone members.

Modifying the members of a Fabric Assist zone

1. Launch the Zone Admin module as described on page 83.
2. Click the **Fabric Assist** tab.
3. Select the FA zone you want to modify from the Name drop-down list.
4. Click an element in the Member Selection List that you want to include in your FA zone, or click an element in the FA Zone Members that you want to delete.
5. Click **Add Member** to add an FA zone member, or click **Remove Member** to remove an FA zone member.

Renaming a Fabric Assist zone

Use the following procedure to change the name of an FA zone.

1. Launch the Zone Admin module as described on page 83.
2. Click the **Fabric Assist** tab.
3. Select the FA Zone you want to rename from the Name drop-down list.
4. Click **Rename**.

   The Rename a Fabric Assist Zone dialog box opens.

5. Enter a new FA zone name and click **OK**.

   The FA zone is renamed in the Zone Admin buffer.

Deleting a Fabric Assist zone

Use the following procedure to delete an FA zone.

1. Launch the Zone Admin module as described on page 83.
2. Click the **Fabric Assist Zone** tab.
3. Select the FA zone you want to delete from the Name drop-down list.
4. Click **Delete**.

   The Confirm Deleting Fabric Assist Zone dialog box opens.

5. Click **Yes**.

   The selected FA zone is deleted from the Zone Admin buffer.

Managing zone configurations

A zone configuration is a group of zones; zoning is enabled on a fabric by enabling a specific configuration. You can specify members of a configuration using the following methods:

- Zone names
- QuickLoop names
- FA zone names

Figure 28 shows a sample zoning database and the relationship between the zone aliases, zones, and zoning configuration. The database contains one zoning configuration, `myconfig`, which contains two zones: Zone A and Zone B. The database also contains four aliases, which are members of Zone A and Zone B. Zone A and Zone B also have additional members other than the aliases.

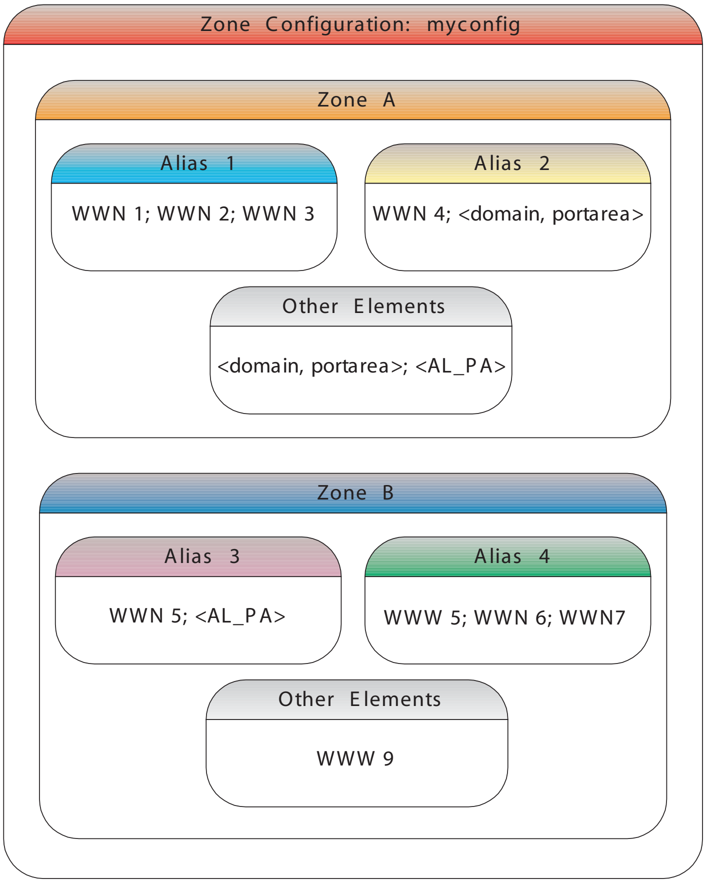


Figure 28 Sample zoning database

Creating a zone configuration

Use the following procedure to create a zone configuration. After creating a zone configuration, you must explicitly enable it for it to take effect.

1. Launch the Zone Admin module as described on page 83.
2. Select a format to display zoning members in the Member Selection List as described in "Zoning views" on page 85.
3. Click the **Config** tab.
4. Click **Create**.

   The Create New Config dialog box appears.
5. Enter a name for the new configuration and click **OK**.

   The new configuration is displayed in the Name list.
6. Click **+** signs in the Member Selection List to view the nested elements.

   The choices available in the list depend on the selection made in the View menu.
7. Highlight an element in the Member Selection List that you want to include in your configuration.

   The Add Member button becomes active.
8. Click **Add Member** to add configuration members.

   Selected members are moved to the Config Members Window.
9. Repeat step 7 and step 8 to add more elements to your configuration.

10. Select **Actions > Save Config Only** to save the configuration changes.

    To enable the configuration, see "Enabling a zone configuration" on page 94.

NOTE: Changes made to the currently enabled configuration do not appear until you reenable the configuration.

Adding or removing zone configuration members

Use the following procedure to add or remove members of a zone configuration.

NOTE: You can make changes to a configuration that is currently enabled; changes do not appear, however, until you reenable the configuration.

Modifying the members of a zone configuration

1. Launch the Zone Admin module as described on page 83.
2. Click the **Config** tab.
3. Select the configuration you want to modify from the Name drop-down list.
4. Click an element in the Member Selection List that you want to include in your configuration or click an element in the Config Members that you want to delete.
5. Click **Add Member** to add a configuration member, or click **Remove Member** to remove a configuration member.
6. Select **Actions > Save Config Only** to save the configuration changes.

   To enable the configuration, see "Enabling a zone configuration" on page 94.

Renaming a zone configuration

Use the following procedure to change the name of a zone configuration.

NOTE: You cannot rename the currently enabled configuration.

1. Launch the Zone Admin module as described on page 83.
2. Click the **Config** tab.
3. Click the configuration you want to rename from the Name drop-down list.
4. Click **Rename**.

   The Rename a Config dialog box opens.
5. Enter a new configuration name and click **OK**.

   The configuration is renamed in the configuration database.
6. Select **Actions > Save Config Only** to save the configuration changes.

   To enable the configuration, see "Enabling a zone configuration" on page 94.

Deleting a zone configuration

Use the following procedure to delete a zone configuration.

NOTE: You cannot delete a currently enabled configuration.

Deleting a disabled configuration

1. Launch the Zone Admin module as described on page 83.
2. Click the **Config** tab.
3. Select the configuration you want to delete from the Name drop-down list.

4. Click **Delete**.

   The Confirm Deleting Config dialog box opens.
5. Click **Yes**.

   The selected configuration is deleted from the configuration database.

Enabling a zone configuration

Several zone configurations can reside on a switch at once, and you can quickly alternate between them. For example, you might want to have one configuration enabled during business hours and another enabled overnight. Only one zone configuration can be enabled at a time, however.

When you enable a zone configuration from Advanced Web Tools, keep in mind that the entire zoning database is saved, and then the selected zone configuration is enabled.

If the zoning database size exceeds the maximum allowed, you cannot enable the zone configuration. The zoning database summary displays the maximum zoning database size (see "Displaying the zone configuration summary" on page 96).

To enable a zone configuration

1. Launch the Zone Admin module as described on page 83.
2. Select **Actions > Enable Config**.

   The Enable Config dialog box opens.
3. Select the configuration to be enabled from the menu.

   A warning is displayed.
4. Click **OK** to save and enable the selected configuration.

Disabling a zone configuration

When you disable the active configuration, the Advanced Zoning feature is disabled on the fabric, and all devices within the fabric can communicate with all other devices. This does not mean that the zoning database is deleted, however, it does mean that there is no configuration active on the fabric.

When you disable a zone configuration from Advanced Web Tools, keep in mind that the entire zoning database is saved, and then the selected zone configuration is disabled.

To disable a zone configuration

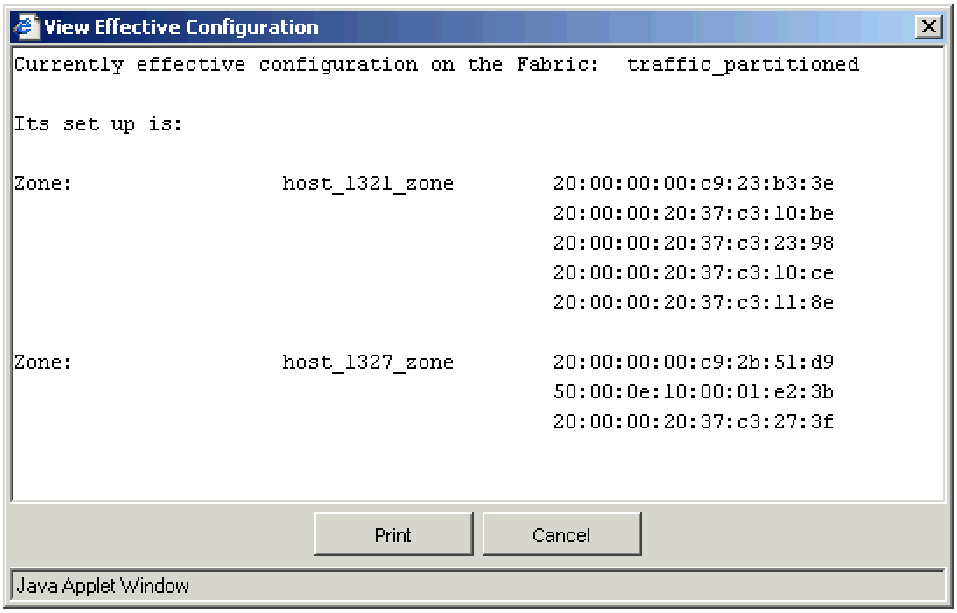
1. Launch the Zone Admin module as described on page 83.
2. Select **Actions > Disable Zoning**.

   The Disable Config warning is displayed.
3. Click **Yes** to save and disable the current configuration.

Displaying the enabled zone configuration

The enabled zone configuration screen displays the actual content of the single zone configuration that is currently enabled on the fabric, and whether it matches the configuration that was enabled when the current zone admin session was launched or last refreshed (see Figure 29). The zones, QuickLoops, and FA zones are displayed, and their contents (ports, WWNs, AL_PAs) are displayed next to them. Aliases are not displayed in the enabled zone configuration. If there is no active zone configuration enabled on the switch, a message is displayed to that effect.

The enabled configuration is listed in the top right corner of the Zone Admin module.



```
Currently effective configuration on the Fabric:  traffic_partitioned

Its set up is:

Zone:                 host_1321_zone        20:00:00:00:c9:23:b3:3e
                                            20:00:00:20:37:c3:10:be
                                            20:00:00:20:37:c3:23:98
                                            20:00:00:20:37:c3:10:ce
                                            20:00:00:20:37:c3:11:8e

Zone:                 host_1327_zone        20:00:00:00:c9:2b:51:d9
                                            50:00:0e:10:00:01:e2:3b
                                            20:00:00:20:37:c3:27:3f
```

Figure 29 Effective Configuration window

Viewing the enabled zone configuration name without launching the Zone Admin module

Select a switch from the Fabric Tree.

The selected switch appears in the Switch View. The current zone configuration name (if one is enabled) is displayed in the lower portion of the Switch Information View. If no zone configuration is enabled, the field displays none.

Viewing detailed information about the enabled zone configuration

1. Launch the Zone Admin module, as described on page 83.

   The zone configuration in effect at the time you launched the Zone Admin module is identified in the top right corner. This information is updated every 15 seconds. It is also updated if you manually refresh the Zone Admin module contents by clicking the refresh icon at the bottom right corner of the Zone Admin module, or when you enable a configuration through the Zone Admin module.

△ **CAUTION:** Clicking the refresh icon overwrites all local unsaved zoning changes. If anyone has made any changes to the zones outside of your Zone Admin session, those changes are applied.

2. Use one of the following methods to identify the most recently effective zone configuration without saving or applying any changes you have made in the Zone Admin module:
   - Select **File > View Effective Configuration** in the Zone Admin module.
   - Click the enabled configuration button in the Zone Admin module.

   Both of these actions display the Effective Configuration window. If no zone is enabled, a message is displayed, indicating that there is no active zoning configuration on the switch.
3. Optional: Click **Print** to print the enabled zone configuration details.

   The print dialog box opens.

Displaying the zone configuration summary

The zone configuration summary hierarchically lists all defined zoning elements known to the current Zone Admin session, whether any of the listed configurations has been enabled, and whether any of the lower level elements has been added as members of the higher level (aliases, zones, QuickLoops, FA zones) structures. The zone configuration summary displays the entire contents of the fabric zoning database as it was at the time the Zone Admin session was launched, or the most recently saved or refreshed information, and any unsaved changes you make since the time the Zone Admin session is launched. It provides the name of the zone configuration that was enabled at the time you launched the Zone Admin session; however, keep in mind that the enabled configuration might have changed since then and that this screen does not reflect those changes.

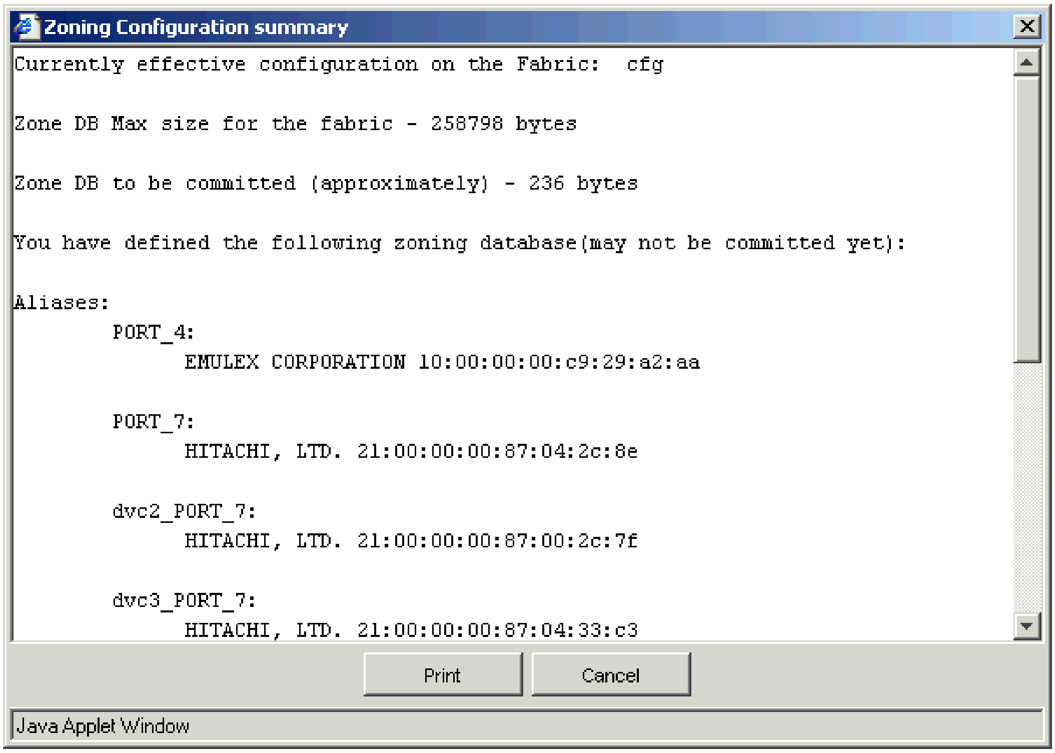
Viewing a zone configuration summary report

1. Launch the Zone Admin module as described on page 83.
2. Select **File > Print Summary**.

   The Zone Configuration summary window is displayed, as shown in Figure 30.

   It is important to note that the summary displays the information based on the changes just made. If current Zone Admin session changes have not yet been saved to the fabric, the information displayed here is different from what is seen from the switch.
3. Optional: Click **Print** to print the zone configuration summary.

   The print dialog box opens.



```
Currently effective configuration on the Fabric:  cfg

Zone DB Max size for the fabric - 258798 bytes

Zone DB to be committed (approximately) - 236 bytes

You have defined the following zoning database(may not be committed yet):

Aliases:
        PORT_4:
              EMULEX CORPORATION 10:00:00:00:c9:29:a2:aa

        PORT_7:
              HITACHI, LTD. 21:00:00:00:87:04:2c:8e

        dvc2_PORT_7:
              HITACHI, LTD. 21:00:00:00:87:00:2c:7f

        dvc3_PORT_7:
              HITACHI, LTD. 21:00:00:00:87:04:33:c3
```

Figure 30 Zone Configuration summary

Creating a configuration analysis report

The configuration analysis report lists the following:

- SAN components (ports, WWNs, and AL_PAs) that are not included in the configuration
- SAN components (ports, WWNs, and AL_PAs) that are contained in the configuration but not in the fabric

To create a configuration analysis report

1. Launch the Zone Admin module as described on page 83.
2. Select the **Config** tab.

3. From the Name drop-down list, select a configuration to be analyzed.
4. Click **Analyze Config**.

   A dialog box opens, asking whether you want to refresh the fabric before running the analysis.
5. Click **Yes** or **No**.

   The configuration analysis window opens.

Displaying Initiator/Target Accessibility Matrix

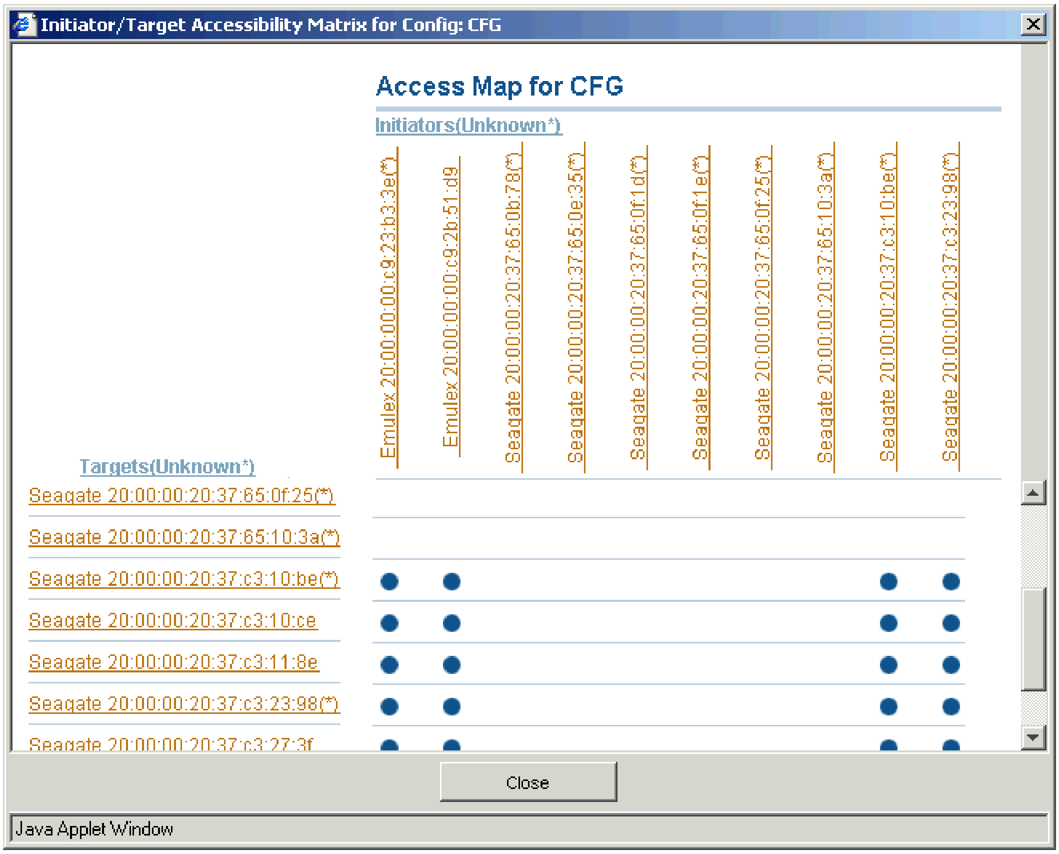
The Initiator/Target Accessibility Matrix shows a list of initiators and a list of targets and indicates which initiator can access which target, as shown in Figure 31.

1. Launch the Zone Admin module as described on page 83.
2. Click the **Config** tab.
3. Select a configuration to be analyzed for device accessibility from the Name drop-down list.
4. Click **Device Accessibility**.

   The Initiator/Target Accessibility Matrix for Config- Device Selection dialog box opens.
5. Select devices you want displayed in the accessibility matrix; select the radio button to select all devices in the fabric or to select a subset of the devices.

   If you select a subset, you must click the devices from the Select Devices list and click **Add** to move them to the Evaluate for Accessibility list.
6. Click **OK**.

   The Initiator/Target Accessibility Matrix opens. You can mouse over a target to display the symbolic name of the device. You can also right-click the device nodes and click **View Device Detail** to display detailed information about the selected device.



Initiator/Target Accessibility Matrix for Config: CFG

Access Map for CFG

Initiators(Unknown*)

Targets(Unknown*)	Emulex 20:00:00:00:c9:23:b3:3e(*)	Emulex 20:00:00:00:c9:2b:51:d9	Seagate 20:00:00:20:37:65:0b:78(*)	Seagate 20:00:00:20:37:65:0e:35(*)	Seagate 20:00:00:20:37:65:0f:1d(*)	Seagate 20:00:00:20:37:65:0f:1e(*)	Seagate 20:00:00:20:37:65:0f:25(*)	Seagate 20:00:00:20:37:65:10:3a(*)	Seagate 20:00:00:20:37:c3:10:be(*)	Seagate 20:00:00:20:37:c3:23:98(*)
Seagate 20:00:00:20:37:65:0f:25(*)										
Seagate 20:00:00:20:37:65:10:3a(*)										
Seagate 20:00:00:20:37:c3:10:be(*)	●	●							●	●
Seagate 20:00:00:20:37:c3:10:ce	●	●							●	●
Seagate 20:00:00:20:37:c3:11:8e	●	●							●	●
Seagate 20:00:00:20:37:c3:23:98(*)	●	●							●	●
Seagate 20:00:00:20:37:c3:27:3f	●	●							●	●

Figure 31 Initiator/Target Accessibility Matrix

Managing the zoning database

This section contains the following procedures for managing the zoning database:

- Adding a WWN to multiple aliases, zones, and Fabric Assist zones, page 98
- Removing a WWN from multiple aliases, zones, and Fabric Assist zones, page 98
- Replacing a WWN in multiple aliases, Fabric Assist zones, and zones, page 98
- Searching for a zone member, page 99
- Clearing the zoning database, page 99
- Adding unzoned online devices to a zone or alias, page 100
- Removing offline devices from the zoning database, page 101
- Replacing offline devices, page 101
- Defining device aliases, page 101

Adding a WWN to multiple aliases, zones, and Fabric Assist zones

This procedure enables you to configure a WWN as a member in a zone configuration prior to adding that device to the fabric. Specifically, it is useful if you want to add a WWN to all or most zoning entities. The added WWN does not need to currently exist in the fabric.

Adding a WWN to the Zone Admin buffer

1. Launch the Zone Admin module as described on page 83.
2. Select **Edit > Add WWN**.

   The Add WWN dialog box opens.
3. Enter a WWN value in the WWN box.
4. Click **OK**.

   The Add WWN dialog box shows all the zoning elements that will include the new WWN, including aliases, zones, and FA zones. All of the elements are selected by default.
5. Click items in the list to select or unselect, and click **Add** to add the new WWN to all the selected zoning elements.

   The WWN is added to the Zone Admin buffer and can be used as a member.

Removing a WWN from multiple aliases, zones, and Fabric Assist zones

This procedure is useful if you want to remove a WWN from all or most zoning entities.

Deleting a WWN from the Zone Admin buffer

1. Launch the Zone Admin module as described on page 83.
2. Select **Edit > Delete WWN**.

   The Delete WWN dialog box opens.
3. Enter a WWN value in the WWN box.
4. Click **OK**.

   The Delete WWN dialog box shows all the zoning elements that include the WWN.
5. Click elements in the list to select or unselect, and then click **Delete** to delete the WWN from all the selected zoning elements.

   The WWN is deleted from the selected items in the Zone Admin buffer.

Replacing a WWN in multiple aliases, Fabric Assist zones, and zones

This procedure enables you to replace a WWN throughout the Zone Admin buffer. This is helpful when exchanging devices in your fabric and helps you to maintain your current configuration.

Replacing a WWN in the Zone Admin buffer

1. Launch the Zone Admin module as described on page 83.
2. Select **Edit > Replace WWN**.

   The Replace WWN dialog box opens.
3. Enter the WWN to be replaced in the Replace box.
4. Enter the new WWN in the By box.
5. Click **OK**.

   The Replace WWN dialog box opens. It lists all the zoning elements that include the WWN.
6. Click elements in the list to select or unselect, and the click **Replace** to replace the WWN in all the selected zoning elements.

   The former WWN is replaced in the Zone Admin buffer by the new WWN, including within any alias or zone in which the old WWN was a member.

Searching for a zone member

You can search zone member selection lists for specified strings of text. If you know some identifying information about a possible member of a zoning entity, you can select the tab and view for that entity and then search through its member selection list using the Search for Zone Member option. If the target entity is an alias, zone, QuickLoop, or FA zone, the search domain includes elements like switch names and domain numbers, port names and domain, port addresses, device WWNs and manufacturer names, and also any aliases that might already have been defined. If the target entity is a configuration, zones, FA zones, and QuickLoops are also included, along with the elements they contain.

The search starts from the top of the list, and when the target element is found, it is also selected in the Member Selection List so it can be added or its parent or children can be found. By default, the Member Selection List is searched from beginning to end one time. If you select the wraparound option, the search continues to loop from the beginning to the end of the Member Selection List.

To search for a zone member

1. Launch the Zone Admin module as described on page 83.
2. Select **Edit > Search Member**.
3. Enter the zone member name in the Member Name field.

   Optional: Narrow the search by selecting one or more of the check boxes, such as **Match Case**.
4. Click **Next** to begin the zone member search.

Clearing the zoning database

Use the following procedure to disable the active zoning configuration, if one exists, and delete the entire zoning database.

△ **CAUTION:** This action not only disables zoning on the fabric, but also deletes the entire zoning database. This results in all devices being able to communicate with each other.

Disabling any active configuration and deleting the entire zoning database

1. Launch the Zone Admin module as described on page 83.
2. Select **Actions > Clear All**.

   The Disable Config warning is displayed.
3. Click **Yes** to do all of the following:
   - Disable the current configuration.
   - Clear the entire contents of the current Zone Admin buffer.
   - Delete the entire persistent contents of the fabric zoning database.

   This action is not recoverable.

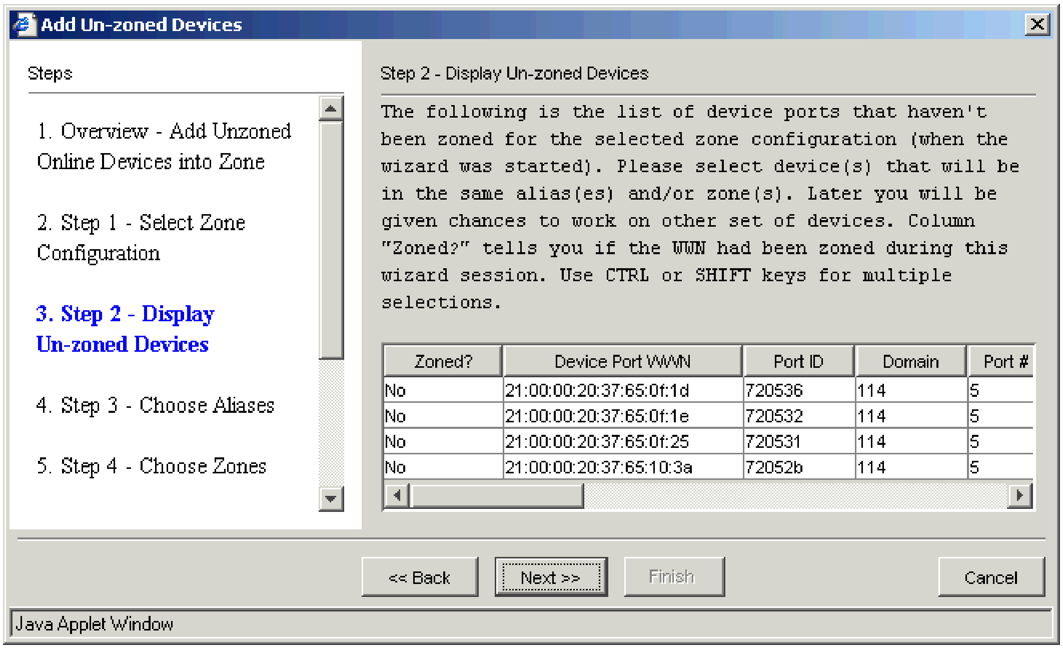
Using zoning wizards

The Zone Admin module contains the following wizards to help you perform the zoning tasks:

- Add Un-zoned Devices
- Remove Offline Devices
- Replace Offline Devices
- Define Device Alias

The wizards are accessed through the Tools menu in the Zone Admin module. The following sections describe the zoning tasks and the procedure for accessing the wizards for each task. The wizards are self-explanatory, so the specific steps are not documented here.

NOTE: The left side of each wizard window lists the steps you need to take to complete the task. The current step is in blue, as shown in Figure 32. Some of the wizards allow you to loop and repeat the task multiple times; as a result, each step is listed in this panel, so that you not only see the steps that you still need to perform, but also the steps that you have already performed. The step numbers may not match the overall numbering in this panel.


Add Un-zoned Devices
Steps
1. Overview - Add Unzoned Online Devices into Zone
2. Step 1 - Select Zone Configuration
3. Step 2 - Display Un-zoned Devices
4. Step 3 - Choose Aliases
5. Step 4 - Choose Zones
<< Back
Next >>
Finish
Cancel
Java Applet Window

Step 2 - Display Un-zoned Devices

```
The following is the list of device ports that haven't
been zoned for the selected zone configuration (when the
wizard was started). Please select device(s) that will be
in the same alias(es) and/or zone(s). Later you will be
given chances to work on other set of devices. Column
"Zoned?" tells you if the WWN had been zoned during this
wizard session. Use CTRL or SHIFT keys for multiple
selections.
```

Zoned?	Device Port WWN	Port ID	Domain	Port #
No	21:00:00:20:37:65:0f:1d	720536	114	5
No	21:00:00:20:37:65:0f:1e	720532	114	5
No	21:00:00:20:37:65:0f:25	720531	114	5
No	21:00:00:20:37:65:10:3a	72052b	114	5

Figure 32 Add Un-zoned Devices wizard

Adding unzoned online devices to a zone or alias

When zoning is enabled, devices that are not included in a zone configuration are inaccessible to other devices in the fabric. Use the following procedure to identify online devices that are not zoned in any zone configuration and add them to a zone or alias.

1. Launch the Zone Admin module as described on page 83.
2. Select **Tools > Add Un-zoned Devices**.

   The Add Un-zoned Devices wizard starts.
3. Follow the steps outlined in the wizard.

   The wizard displays unzoned devices and prompts you to select them and add them to an alias or a zone.

When you have finished the steps for adding a device to a zone or alias, if there are any more unzoned devices, you can either continue to add those unzoned devices or exit the wizard. If there are no more unzoned devices, you must exit the wizard.

Removing offline devices from the zoning database

Removing offline devices (WWNs) helps clean the zoning database to save more space for new entries. Use the following procedure to view all devices that are no longer online and remove all or selected offline devices from the zoning database.

1. Launch the Zone Admin module as described on page 83.
2. Select **Tools > Remove Offline Devices**.

   The Remove Offline Devices wizard starts.
3. Follow the steps outlined in the wizard.

   The wizard allows you to view all devices that are no longer online, and remove all or selected offline devices from the zoning database.

Replacing offline devices

Replacing an offline device replaces its WWN with a new given WWN in all of aliases and zones that contain it. Use the following procedure to view offline devices and replace them with new ones in the zoning database.

1. Launch the Zone Admin module as described on page 83.
2. Select **Tools > Replace Offline Devices**.

   The Replace Offline Devices wizard starts.
3. Follow the steps outlined in the wizard.

   The wizard allows you to view all devices that are no longer online, and replace all or selected offline devices with new ones (WWNs) in the zoning database.

Defining device aliases

Use the following procedure to define zone alias names for devices in a single process. This procedure is especially useful if you use one unique zone alias to name each device port.

The alias definitions of the devices are saved in the zoning database on the switch, which has a size limit. If database size becomes a concern, reconsider your use of alias definitions.

Assigning aliases to devices

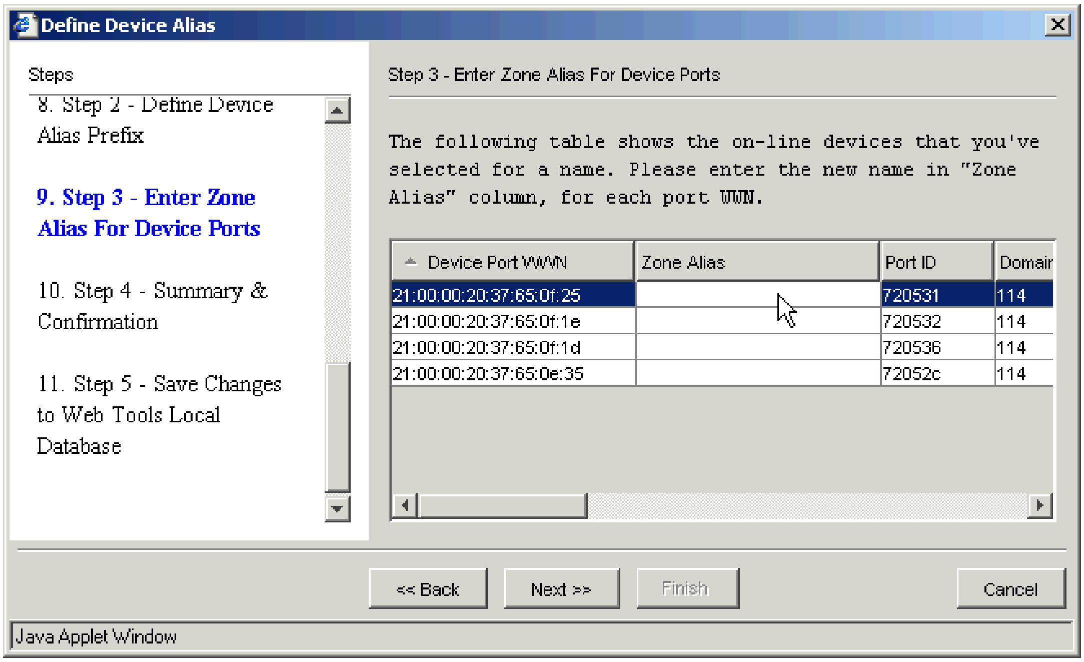
1. Launch the Zone Admin module as described on page 83.
2. Select **Tools > Remove Offline Devices**.

   The Define Device Alias wizard starts.
3. Follow the steps outlined in the wizard.

   The wizard allows you to define one and only one name for each device port (WWN). Devices with one or more aliases are considered already named and are not displayed.

NOTE: To enter a zone alias name, double-click the **Zone Alias** box for each device, as shown in Figure 33, and enter the name.

After entering each alias name, you must press Enter or click another Zone Alias field, or the wizard does not accept the name.


Define Device Alias
Steps
8. Step 2 - Define Device Alias Prefix
9. Step 3 - Enter Zone Alias For Device Ports
10. Step 4 - Summary & Confirmation
11. Step 5 - Save Changes to Web Tools Local Database
Step 3 - Enter Zone Alias For Device Ports
<< Back
Next >>
Finish
Cancel
Java Applet Window

The following table shows the on-line devices that you've selected for a name. Please enter the new name in "Zone Alias" column, for each port WWN.

Device Port WWN	Zone Alias	Port ID	Domain
21:00:00:20:37:65:0f:25		720531	114
21:00:00:20:37:65:0f:1e		720532	114
21:00:00:20:37:65:0f:1d		720536	114
21:00:00:20:37:65:0e:35		72052c	114

Figure 33 Entering a zone alias in the Define Device Alias wizard

Best practices for zoning

Following are recommendations when using zoning:

- Always zone using the highest Fabric OS-level switch.
- Zone using the core switch versus an edge switch.
- Zone using a director versus a switch.
- Zone on the switch you connect to when bringing up Advanced Web Tools (the proxy switch).

10 Working with diagnostic features

This chapter contains the following information:

Managing trace dumps

A trace dump is a snapshot of the running behavior within the HP StorageWorks switch. The dump can be used by developers and troubleshooters at HP to help understand what might be contributing to a specific switch behavior when certain internal events are seen. For example, a trace dump can be created each time a certain error message is logged to the system error log. Developers can then examine what led up to the message event by studying the traces.

Tracing is always on. As software on the switch executes, the trace information is placed into a circular buffer in system RAM. Periodically, the trace buffer is frozen and saved. This saved information is called a *trace dump*.

A trace dump is generated when:

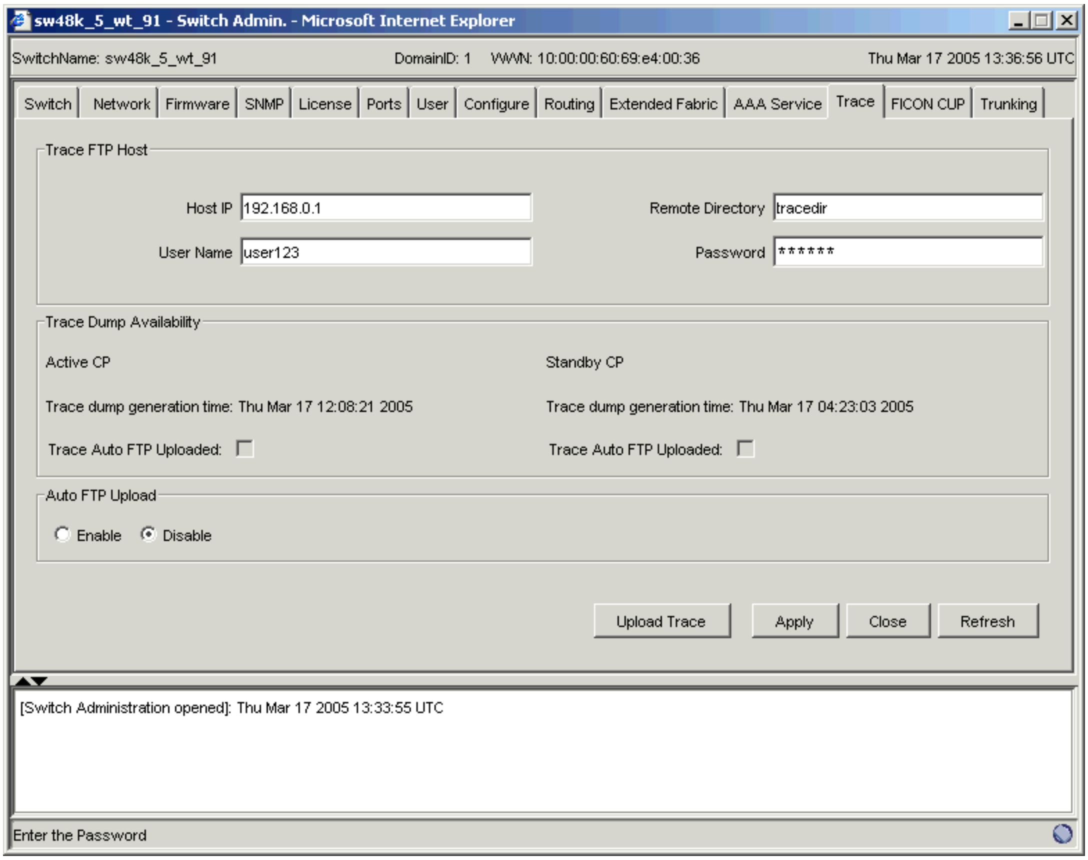
- It is triggered manually (use the `traceDump` command)
- A critical-level LOG message occurs
- A particular LOG message occurs (use the `traceTrig` command to set up the conditions for this)
- A kernel panic occurs
- The hardware watchdog timer expires

(For information about the `traceDump` and `traceTrig` commands, see the *HP StorageWorks Fabric OS 5.x command reference guide*.)

The trace dump is maintained on the switch until either it is uploaded to the FTP host or another trace dump is generated. If another trace dump is generated before the previous one is uploaded, the previous dump is overwritten.

When a trace dump is generated, it is uploaded to an FTP host if automatic FTP uploading is enabled.

Using the Trace tab of the Switch Admin module, you can view and configure the trace FTP host target, enable or disable automatic trace uploads, and manually upload a trace dump (see Figure 34).



sw48k_5_wt_91 - Switch Admin. - Microsoft Internet Explorer

SwitchName: sw48k_5_wt_91 DomainID: 1 WWN: 10:00:00:60:69:e4:00:36 Thu Mar 17 2005 13:36:56 UTC

Trace FTP Host

Host IP 192.168.0.1

Remote Directory tracedir

User Name user123

Password ******

Trace Dump Availability

Active CP

Trace dump generation time: Thu Mar 17 12:08:21 2005

Trace Auto FTP Uploaded: □

Standby CP

Trace dump generation time: Thu Mar 17 04:23:03 2005

Trace Auto FTP Uploaded: □

Auto FTP Upload

○ Enable ● Disable

[Switch Administration opened]: Thu Mar 17 2005 13:33:55 UTC

Enter the Password

Figure 34 Trace tab

How a trace dump is used

The generation of a trace dump causes a CRITICAL message to be logged to the system error log. When a trace dump is detected, issue the `supportSave` command on the affected switch. This command packages all error logs, the `supportShow` output, and the trace dump, and moves these to your FTP server. You can also configure your switch to copy trace dumps to your FTP server (see"Setting up automatic trace dump transfers" next).

In addition to automatic generation of trace dumps on faults, you can also generate a trace dump manually or when certain system error messages are logged. This is normally done with assistance from HP customer support when diagnosing switch behavior.

For details on the commands, see the *HP StorageWorks Fabric OS 5.x command reference guide*.

Setting up automatic trace dump transfers

You can set up a switch so that diagnostic information is transferred to a remote server. Then, if a problem occurs you can provide your customer support representative with the most detailed information possible. To ensure the best service, you should set up for automatic transfer as part of standard switch configuration, before a problem occurs.

Setting up for automatic transfer of diagnostic files involves the following tasks:

- Specify a remote server to store the files.
- Enable the automatic transfer of trace dumps to the server. (Trace dumps overwrite each other by default; sending them to a server preserves information that would otherwise be lost.)

You should also set up a periodic checking of the remote server so that you are alerted if the server becomes unavailable and you can correct the problem. See the *HP StorageWorks Fabric OS 5.x administrator guide* for additional information.

The following procedures describe in detail the tasks for setting up automatic transfer.

Specifying a remote server

1. Launch the Switch Admin module as described on page 36.
2. Click the **Trace** tab.
3. Enter the FTP host IP address, path of the remote directory in which to store the trace dump files, FTP user name, and FTP password in the appropriate fields.

   The password is optional if you log in as an anonymous user.
4. Click **Apply**.

Enabling automatic transfer of trace dumps

1. Launch the Switch Admin module as described on page 36.
2. Click the **Trace** tab.
3. Click **Enable** in the Auto FTP Upload section to enable automatic uploading of the trace dump to the FTP host.
4. Click **Apply**.

Disabling automatic trace uploads

If automatic uploading of a trace dump is disabled, you must manually upload the trace dump or else the information is overwritten when a subsequent trace dump is generated.

Disabling automatic uploading of the trace dump

1. Launch the Switch Admin module as described on page 36.
2. Click the **Trace** tab.
3. Click **Disable** in the Auto FTP Upload section to disable automatic uploading of the trace dump to the FTP host.
4. Click **Apply**.

Uploading a trace dump manually

You can manually upload a trace dump when automatic uploading is not enabled.

Uploading a trace dump

1. Launch the Switch Admin module as described on page 36.
2. Click the **Trace** tab.

   The Trace Dump Availability section shows whether a trace dump is available. If the Trace Auto FTP Uploaded box is selected, the trace dump has been uploaded to the FTP host.
3. Click **Upload Trace** (if the Upload Trace button is inactivated, it means that a trace dump is not available).

   The Upload Trace dialog box opens, along with the default trace dump file name.
4. Optional: Enter a new trace dump file name if you want to change it from the default name.
5. For the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director only, click the CP (active or standby) from which the trace dump is to be uploaded.

   If the CP does not have a trace dump, that CP selection is disabled.
6. Click **OK**.

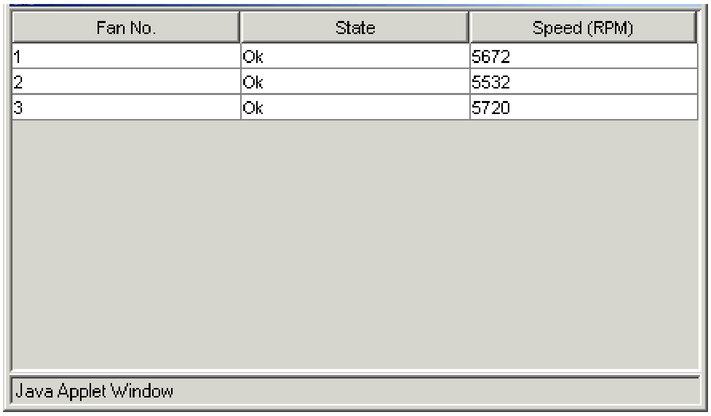
Displaying switch information

This section describes how to display information about the physical components of the switch (such as fan, temperature, and power supply) as well as how to display other detailed switch information (such as firmware and IP address).

Displaying detailed fan hardware status

The background color of the Fan button indicates the overall status of the fans. For more information about the switch fan, see the appropriate hardware documentation.

You can display status information about the fans, as shown in Figure 35.



Fan No.	State	Speed (RPM)
1	Ok	5672
2	Ok	5532
3	Ok	5720

Java Applet Window

Figure 35 Fan status window

Note that the Fan No. column indicates either the fan number or the fan FRU number, depending on the switch model. A fan FRU can contain one or more fans.

- For the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director and the SAN Switch 4/32, the Fan No. column indicates the fan FRU number.
- For the SAN Switch 2/32, the Fan No. column indicates the fan number.
- The 4Gb SAN Switch for HP p-Class BladeSystem, 4/16 SAN Switch, SAN Switch 2/8V, and SAN Switch 2/16V do not contain fan FRUs, so for these switch models, the Fan No. column indicates the fan number.

Displaying the fan status detail

1. Select a switch from the Fabric Toolbar.

   The selected switch appears in the Switch View.
2. Click the **Fan** button on the Switch View.

   The detailed fan status for the switch is displayed, as shown in Figure 36.

Displaying the temperature status

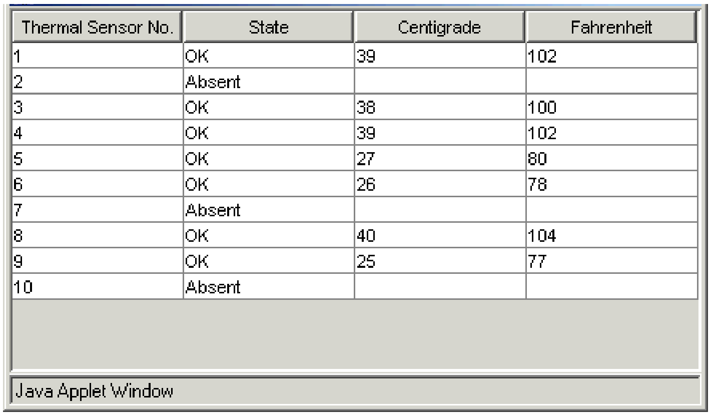
The background color of the Temp button indicates the overall status of the temperature. For more information regarding switch temperature, see the appropriate switch or director documentation.

Displaying the temperature status detail

1. Select a switch from the Fabric Toolbar.

   The selected switch appears in the Switch View.
2. Click the **Temp** button on the Switch View.

   The detailed temperature sensor states for the switch are displayed, as shown in Figure 37 on page 108.



Thermal Sensor No.	State	Centigrade	Fahrenheit
1	OK	39	102
2	Absent		
3	OK	38	100
4	OK	39	102
5	OK	27	80
6	OK	26	78
7	Absent		
8	OK	40	104
9	OK	25	77
10	Absent		

Figure 36 Temperature status window

Displaying the power supply status

The background color of the Power button indicates the overall status of the power supply modules. For more information regarding switch power modules, see the appropriate hardware documentation.

Displaying the power supply status detail

1. Select a switch from the Fabric Tree.

   The selected switch appears in the Switch View.

2. Click the **Power** button on the Switch View.

   The detailed power supply states are displayed for the switch.

Checking the physical health of a switch

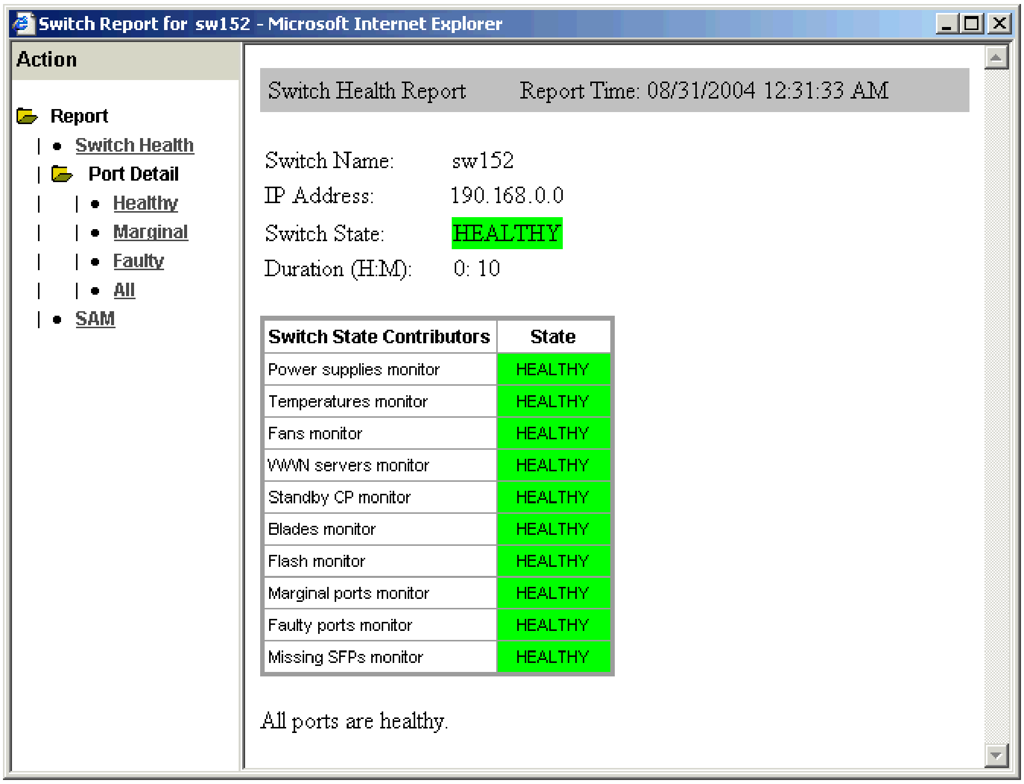
The Status button displays the operational state of the switch. The background color of the button displays the real-time status of the switch. See the Status Legend for the meaning of the background colors.

If no data is available from a switch, the most recent background color remains displayed.

For all statuses that are based on errors per time interval, any errors cause the status to show faulty until the entire sample interval has passed.

If the switch status is marginal or critical, information on the trigger that caused that status is displayed in the Switch Information view.

Click the **Status** button to display a detailed, customizable switch status report, as shown in Figure 37. Note that this is a static report and not a dynamic view of the switch.



Switch Health Report Report Time: 08/31/2004 12:31:33 AM

Switch Name: sw152
IP Address: 190.168.0.0
Switch State: HEALTHY
Duration (H:M): 0: 10

Switch State Contributors	State
Power supplies monitor	HEALTHY
Temperatures monitor	HEALTHY
Fans monitor	HEALTHY
WWN servers monitor	HEALTHY
Standby CP monitor	HEALTHY
Blades monitor	HEALTHY
Flash monitor	HEALTHY
Marginal ports monitor	HEALTHY
Faulty ports monitor	HEALTHY
Missing SFPs monitor	HEALTHY

All ports are healthy.

Figure 37 Switch report

Displaying a detailed switch status report

1. Select a switch from the Fabric Tree.

   The selected switch appears in the Switch View.

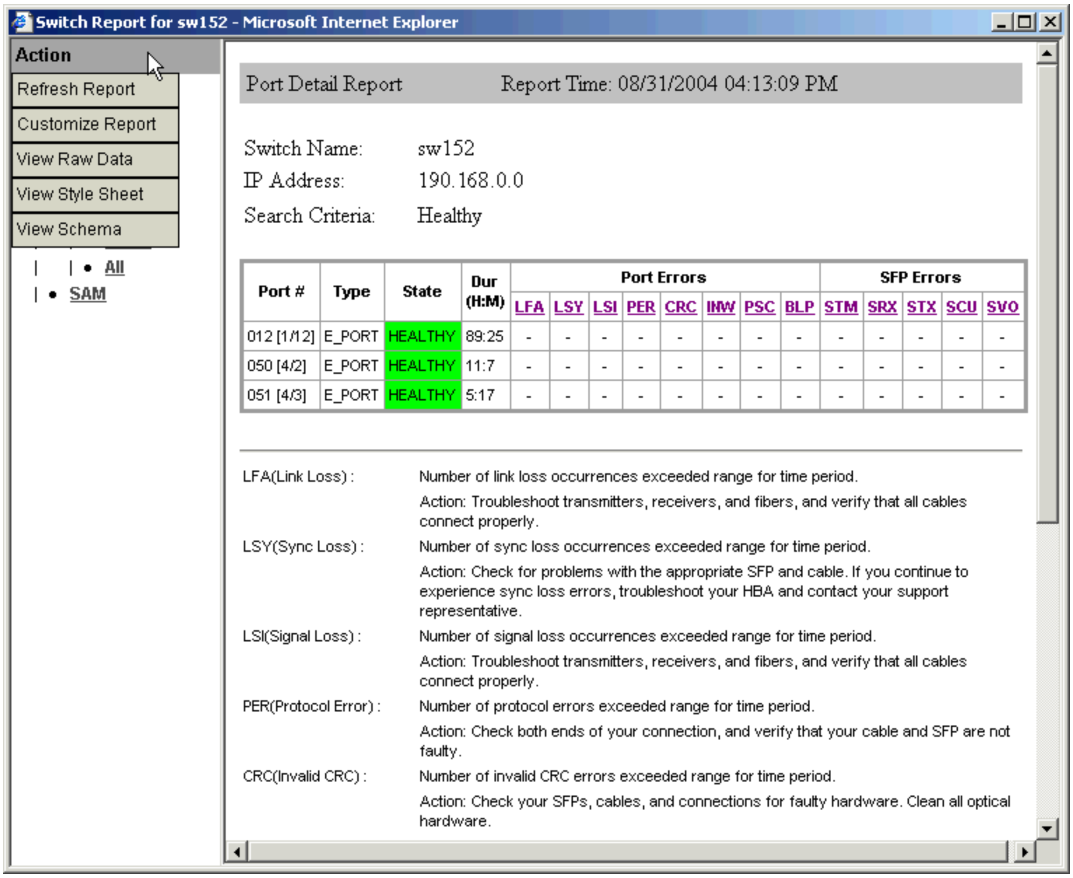
2. Click the **Status** button on the Switch View.

   The detailed switch health report is displayed, as shown in Figure 37.

3. Optional: Click the underlined links in the left panel to display detailed information about ports and Switch Availability Monitoring (SAM).

4. Optional: Mouse-over the **Action** box (see Figure 38) and click an action to:

   - Refresh the information displayed in the report
   - Customize the report
   - View the data in raw XML format
   - View the style sheet for the report
   - View the XML schema for the report



Port Detail Report Report Time: 08/31/2004 04:13:09 PM

Switch Name: sw152
IP Address: 190.168.0.0
Search Criteria: Healthy

Port #	Type	State	Dur (H:M)	Port Errors								SFP Errors				
				LFA	LSY	LSI	PER	CRC	INW	PSC	BLP	STM	SRX	STX	SCU	SVO
012 [1/12]	E_PORT	HEALTHY	89:25	-	-	-	-	-	-	-	-	-	-	-	-	-
050 [4/2]	E_PORT	HEALTHY	11:7	-	-	-	-	-	-	-	-	-	-	-	-	-
051 [4/3]	E_PORT	HEALTHY	5:17	-	-	-	-	-	-	-	-	-	-	-	-	-

LFA(Link Loss) : Number of link loss occurrences exceeded range for time period.
Action: Troubleshoot transmitters, receivers, and fibers, and verify that all cables connect properly.

LSY(Sync Loss) : Number of sync loss occurrences exceeded range for time period.
Action: Check for problems with the appropriate SFP and cable. If you continue to experience sync loss errors, troubleshoot your HBA and contact your support representative.

LSI(Signal Loss) : Number of signal loss occurrences exceeded range for time period.
Action: Troubleshoot transmitters, receivers, and fibers, and verify that all cables connect properly.

PER(Protocol Error) : Number of protocol errors exceeded range for time period.
Action: Check both ends of your connection, and verify that your cable and SFP are not faulty.

CRC(Invalid CRC) : Number of invalid CRC errors exceeded range for time period.
Action: Check your SFPs, cables, and connections for faulty hardware. Clean all optical hardware.

Figure 38 Switch report action menu

Interpreting port LEDs

The Switch View displays port graphics with blinking LEDs, simulating the physical appearance of the ports. One of the LEDs indicates port status; the other indicates port speed. For LED information, see the hardware documentation for the switch you are viewing.

The background color of the port icon indicates the port status, as follows:

- Green (healthy)
- Yellow (marginal)
- Red (critical)
- Gray (unmonitored)

If the entire port icon is blue, the port is buffer-limited.

If a group of port icons is grayed out, those ports are not licensed.

The port status is also indicated in the Port Information screen in the Port Health box for the selected port. (See Figure 41 on page 111.)

Figure 39 shows a port icon and associated LEDs from a Core Switch 2/64. The port icons are different for different switch models.

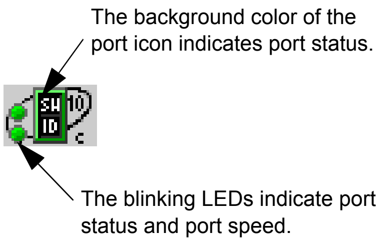

The background color of the port icon indicates port status.
The blinking LEDs indicate port status and port speed.

Figure 39 Port and LED status color-coded information

For the 4/256 SAN Director, the representation of the port LEDs on the FC4-32 port blade is not the same as the LEDs on the physical blade. Figure 40 compares the LEDs on the physical port card and the Advanced Web Tools display.

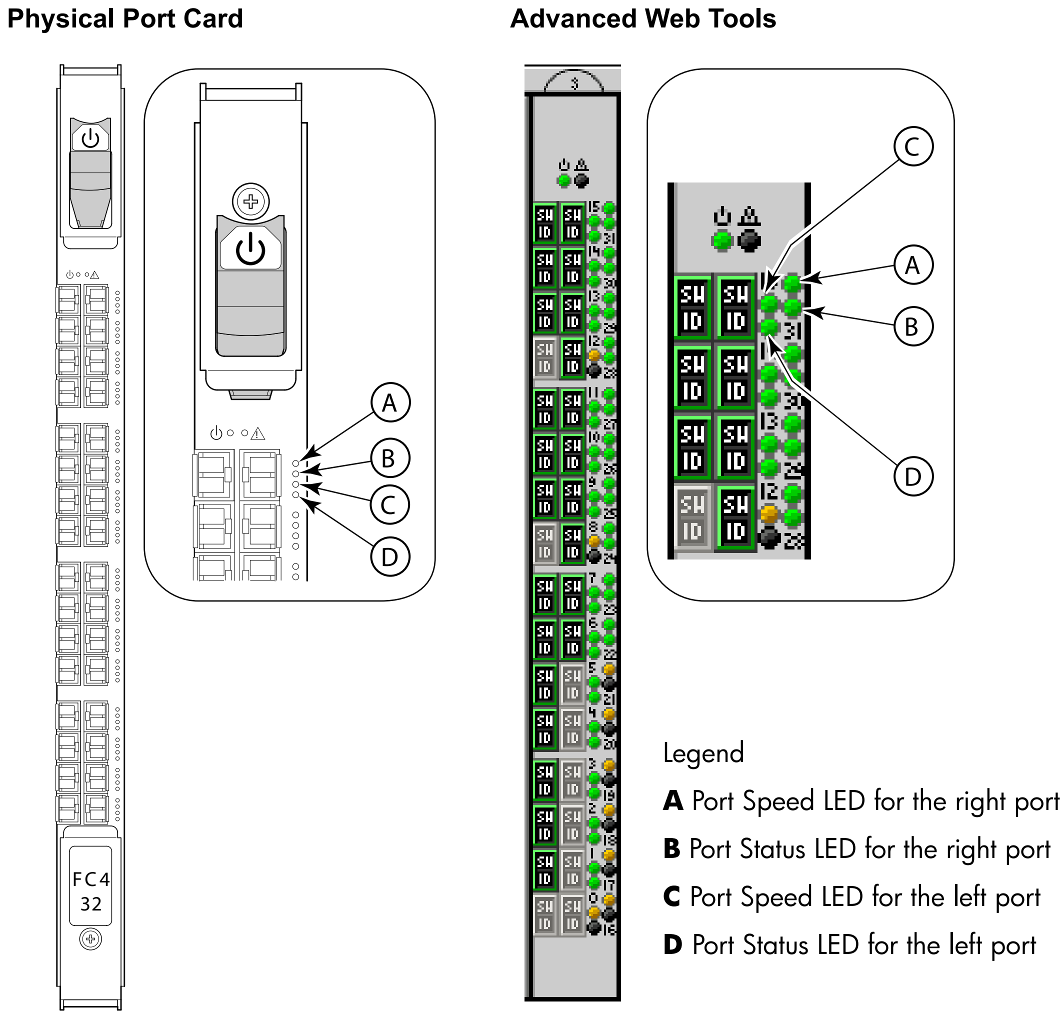
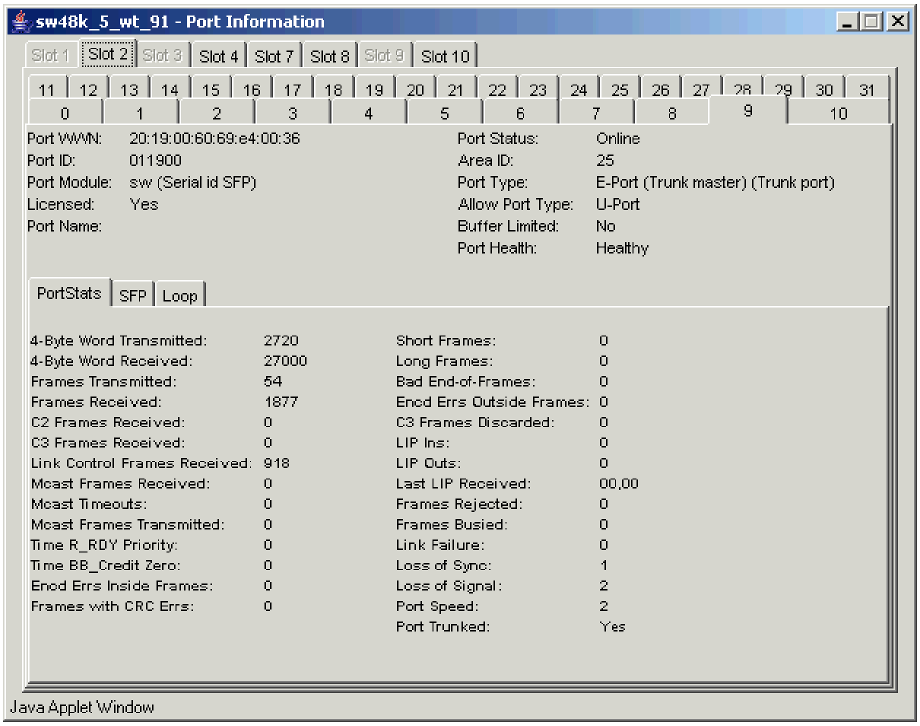

Physical Port Card
Advanced Web Tools
FC4
32
A
B
C
D
Legend
A Port Speed LED for the right port
B Port Status LED for the right port
C Port Speed LED for the left port
D Port Status LED for the left port

Figure 40 Port LEDs for the FC4-32 port blade in the 4/256 SAN Director

Displaying port information

The Port Information screen displays statistics and status for the selected port, SFP, or loop, as shown in Figure 41. Access the Port Information screen by clicking any of the ports in the Switch View.



Port WWN:	20:19:00:60:69:e4:00:36	Port Status:	Online
Port ID:	011900	Area ID:	25
Port Module:	sw (Serial id SFP)	Port Type:	E-Port (Trunk master) (Trunk port)
Licensed:	Yes	Allow Port Type:	U-Port
Port Name:		Buffer Limited:	No
		Port Health:	Healthy

4-Byte Word Transmitted:	2720	Short Frames:	0
4-Byte Word Received:	27000	Long Frames:	0
Frames Transmitted:	54	Bad End-of-Frames:	0
Frames Received:	1877	Encd Errs Outside Frames:	0
C2 Frames Received:	0	C3 Frames Discarded:	0
C3 Frames Received:	0	LIP Ins:	0
Link Control Frames Received:	918	LIP Outs:	0
Mcast Frames Received:	0	Last LIP Received:	00,00
Mcast Timeouts:	0	Frames Rejected:	0
Mcast Frames Transmitted:	0	Frames Busied:	0
Time R_RDY Priority:	0	Link Failure:	0
Time BB_Credit Zero:	0	Loss of Sync:	1
Encd Errs Inside Frames:	0	Loss of Signal:	2
Frames with CRC Errs:	0	Port Speed:	2
		Port Trunked:	Yes

Figure 41 Port information screen

The number of slots displayed in the Port Information screen depends on the switch model. For example, each logical switch in the Core Switch 2/64 (and the SAN Director 2/128 and 4/256 SAN Director, if configured for two logical switches) has four slots. For these switch types, a subtab is displayed for each physically inserted and powered on slot in the Port Information screen. You must first click the slot tab and then the port tab for that slot.

For the 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, 4Gb SAN Switch for HP p-Class BladeSystem, and SAN Switch 4/32, there are no subtabs for the slots. There is just a port tab for each port.

The Port Information screen displays two values relating to port type, which are defined as follows:

- Port Type, which is the actual or current port type. If the port is offline, this value is the allowed types (or U-Port, if no type constraint has been specified). If the port is online, this value is the type the port has actually negotiated to.
- Allow Port Type, which is the allowed or configured port type, as set by the type check boxes in the Switch Admin module, Ports tab. (See "Configuring port type" on page 45 for more information.)

Accessing the Port Information screen

1. Select a switch from the Fabric Tree.

   The selected switch is displayed in the Switch View.
2. Click the port icon for which you want to view information.

   The Port Information screen is displayed.
3. Perform the following, according to switch type:

- For Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, click the slot tab that corresponds to the correct slot for the logical switch.
- For 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, 4Gb SAN Switch for HP p-Class BladeSystem, and SAN Switch 4/32, proceed directly to the next step.

4. Click the **Port** tab.
5. Optional: To view additional port information, select one of the subtabs for each port: **PortStats**, **SFP**, or **Loop**.

11 Administering FICON CUP fabrics

NOTE: FICON is not supported on HP B-Series Fibre Channel switches. The FICON information in this document is included for reference only.

This chapter contains the following sections:

Control Unit Port (CUP) is a protocol for managing FICON directors. Host-based management programs manage the switches using CUP protocol by sending commands to the emulated Control Device implemented by Fabric OS. A switch or director that supports CUP can be controlled by one or more host-based management programs or director consoles. The director allows control to be shared between host-based management programs and director consoles.

To use FICON CUP, you must:

- Install a FICON CUP license on a FICON director
- Enable FMS mode on the FICON director
- Configure CUP attributes (FMS parameters) for the FICON director

All of these things can be done using Advanced Web Tools. You can also use Advanced Web Tools to manage FICON directors (when FMS mode is enabled on those directors) to:

- Display the control device state
- Display a code page
- Manage port connectivity configuration

You do not need to install the FICON CUP license to perform FICON CUP management; you must install the FICON CUP license, however, if your switch is to enforce traffic between the FICON director and the host-based management program.

Enabling or disabling FMS mode

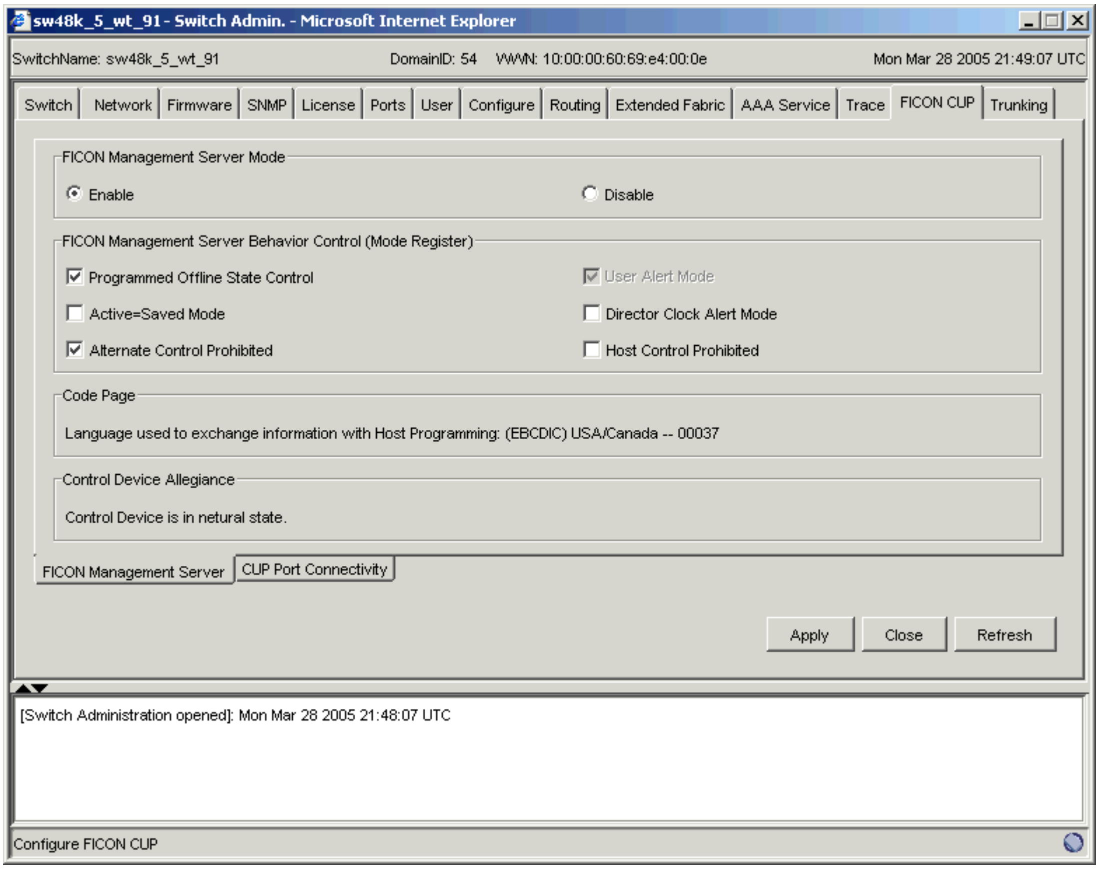
FICON Management Server (FMS) is used to support switch management using CUP. To be able to use the CUP functionality, all switches in the fabric must have FMS mode enabled. FMS mode is a per-switch setting. After FMS mode is enabled, you can activate a CUP license without rebooting the director. You can use Advanced Web Tools to install a CUP license. For more information on installing licenses, see ”Activating a license on a switch” on page 48.

When FMS mode is disabled, mainframe management applications, director consoles, or alternate managers cannot communicate with a director with CUP. In addition, when FMS mode is disabled on a director, you cannot configure CUP attributes.

To enable or disable FMS mode

1. Click a FICON CUP-capable switch from the Fabric Tree.
2. Launch the Switch Admin module as described on page 36.
3. Click the **FICON CUP** tab.

   The FICON CUP tabbed page is displayed, with the FMS subtabbed page in front, as shown in Figure 42. All attributes on this tab are disabled until FMS mode is enabled.
4. Select the **Enable** radio button to enable FMS mode.



SwitchName: sw48k_5_wt_91 DomainID: 54 WWN: 10:00:00:60:69:e4:00:0e Mon Mar 28 2005 21:49:07 UTC

FICON Management Server Mode

● Enable ○ Disable

FICON Management Server Behavior Control (Mode Register)

☑ Programmed Offline State Control ☑ User Alert Mode

□ Active=Saved Mode □ Director Clock Alert Mode

☑ Alternate Control Prohibited □ Host Control Prohibited

Code Page

Language used to exchange information with Host Programming: (EBCDIC) USA/Canada -- 00037

Control Device Allegiance

Control Device is in netural state.

[Switch Administration opened]: Mon Mar 28 2005 21:48:07 UTC

Configure FICON CUP

Figure 42 FICON CUP management

Configuring FMS parameters

FMS parameters control the behavior of the switch with respect to CUP itself, as well as the behavior of other management interfaces (director console, alternate managers). You can configure FMS parameters for a switch only after FMS mode is enabled on the switch. All FMS parameter settings are persistent across switch power cycles. There are six FMS parameters, as described in Table 10.

Table 10 FMS mode paramenter descriptions

Parameter	Description
Programmed Offline State Control	This parameter controls whether host programming is allowed to set the switch offline. The parameter is enabled by the hardware after system installation, and can be reset by Advanced Web Tools.
Active=Saved Mode	This parameter controls the IPL file update. The IPL file saves port connectivity attributes and port names. After a switch reboot or power cycle, the switch reads the IPL file and actives its contents as default configuration. When this mode is enabled, activating a configuration saves a copy to the IPL configuration file. All changes made to the active connectivity attributes or port names by host programming or alternate managers are saved in this IPL file. This mode keeps the current active configuration persistent across switch reboots and power cycles. You cannot directly modify the IPL file or save a file as an IPL file. When this mode is disabled, the IPL file is not altered for either new configuration activation or any changes made on the current active configuration. This mode is set as enabled by the hardware after system installation, and can be reset by Advanced Web Tools. **NOTE:** When FMS mode is enabled and the Active=Saved mode is disabled, you can enable and disable ports, but the setting is not persistent. When the Active=Saved mode is enabled, you can enable and disable ports and the setting is persistent.
Alternate Control Prohibited	This parameter determines whether alternate managers are allowed to modify port connectivity. Enabling this mode prohibits alternate manager control of port connectivity; otherwise, alternate managers can manage port connectivity. This parameter is enabled by the hardware after system installation, and can be reset by Advanced Web Tools.
User Alert Mode	This mode controls director console behavior for alerts. Enabling this mode prompts the director consoles to display a warning whenever you attempt an action that will change switch parameters. When you disable this mode, no warning is displayed. In this case, in which Advanced Web Tools is the director console, warning messages are displayed by Advanced Web Tools regardless of the setting of the mode, since Advanced Web Tools always displays warning messages when you apply a change to a switch that changes mode. This mode is always read-only in Advanced Web Tools. Each time that the switch is powered on, the mode is reset to disabled.
Director Clock Alert Mode	This mode controls behavior for attempts to set the switch timestamp clock through the director console. When it is enabled, the director console (Advanced Web Tools, in this case) displays warning indications when the switch timestamp is changed by a user application. When it is disabled, you can activate a function to set the timestamp clock. There is no indication for timestamp clock setting. This mode is set as disabled by the hardware after system installation, and can be reset by Advanced Web Tools.
Host Control Prohibited	This mode determines whether host programming allows modifying port connectivity. Enabling this mode prohibits host programming control of port connectivity; otherwise, host programming can manage port connectivity. This mode is set as disabled by the hardware after system installation. and can be reset by Advanced Web Tools.

Configuring FMS mode parameters

1. Click a FICON-enabled switch from the Fabric Tree.
2. Launch the Switch Admin module as described on page 36.
3. Click the **FICON CUP** tab.

   The FICON CUP tabbed page is displayed, with the FMS subtabbed page in front (see Figure 42 on page 114). All attributes on this tab are read-only until FMS mode is enabled.
4. To enable or disable an FMS mode parameter, select the check box next to the parameter. A selected check box means that the parameter is enabled. You cannot configure the User Alert Mode parameter in Advanced Web Tools, as it is read-only.

Displaying the code page information

The Code Page box identifies the language used to exchange information between the FICON director and Host Programming. It is a read-only field in Advanced Web Tools; it is set only by Host Programming. When FMS mode is disabled, the code page is displayed as unavailable.

1. Click a FICON-enabled switch from the Fabric Tree.
2. Launch the Switch Admin module as described on page 36.
3. Click the **FICON CUP** tab.

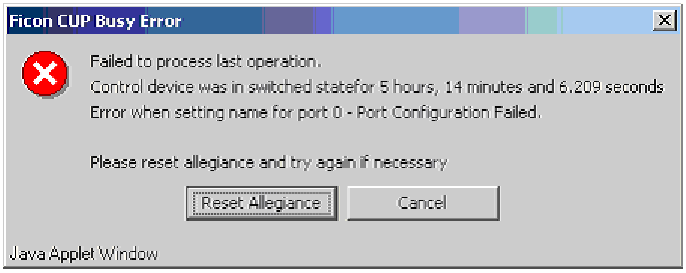
   The FICON CUP tabbed page is displayed, with the FMS subtabbed page in front (see Figure 42 on page 114). All attributes on this tab are read-only until FMS mode is enabled.

   The code page format is displayed in the Code Page box. For example:

```
Language used to exchange information with Host Programming: (EBCDIC)
USA/Canada -- 00037
```

Displaying the Control Device state

The Control Device is in either a neutral or a switched state. When it is neutral, the Control Device accepts commands from any channel that has established a logic path with it and accepts commands from alternate managers. When the Control Device is switched, it establishes a logical path and accepts commands only from that logical path (device allegiance). Commands from other paths cause a FICON CUP Busy Error (see Figure 43). Most write operations from alternate managers are also rejected.



Failed to process last operation.
Control device was in switched statefor 5 hours, 14 minutes and 6.209 seconds
Error when setting name for port 0 - Port Configuration Failed.

Please reset allegiance and try again if necessary

Figure 43 FICON CUP busy error

Device allegiance usually lasts for a very short time. However, under abnormal conditions, device allegiance can get stuck and fail to terminate. It might cause the switch to be unmanageable with CUP, and you will continue to receive the FICON CUP Busy Error. In this case, you should check the Control Device state and the last update time to determine whether the device allegiance is stuck. The Advanced Web Tools Switch Admin displays the Control Device state and last update time (see Figure 42 on page 114). You can click Refresh to get most recent update.

You can manually reset allegiance to bring the Control Device back to the neutral state by clicking Reset Allegiance in the FICON CUP Busy Error display (see Figure 43).

The FICON CUP Busy Error can be caused by the following switch parameters being read or modified:

- Mode Register
- Port Names (also called Port Address Name)
- PDCM and Port Connectivity Attributes
- Switch enable/disable
- Switch name change

Displaying the Control Device state

1. Click a FICON-enabled switch from the Fabric Tree.
2. Launch the Switch Admin module as described on page 36.
3. Click the **FICON CUP** tab.

   The FICON CUP tabbed page is displayed, with the FMS subtabbed page in front (see Figure 42 on page 114). All attributes on this tab are read-only until FMS Mode is enabled.

   The Control Device state is displayed as neutral or switched in the Control Device Allegiance box.

   If FMS mode is enabled, and the Control Device state is unavailable, the FICON CUP Busy Error is displayed.
4. Click **Reset Allegiance** in the error message to reset the Control Device state to its correct state (see Figure 43 on page 116).

Configuring CUP port connectivity

In the Port Connectivity subpanel (shown in Figure 44), you can manage the configuration files and active configuration. All CUP configuration files and the active configurations are listed in a table. The active configuration is listed as `Active Configuration*` and the description in the table is `Current active configuration on switch`. The other special configuration file is the IPL. Any other files displayed are user-defined configurations and are stored on the switch.

You can create, activate, copy, or delete saved CUP port connectivity configurations; however, you can edit or copy a configuration only while it is active. You can also activate, edit, or copy the IPL configuration. You must have FMS mode enabled before you can make any changes to the configurations. Click **Refresh** to get the latest configuration file list from the switch.

When creating a new configuration or editing an existing configuration, keep in mind that Advanced Web Tools port name input is restricted to printable ASCII characters. Therefore, when Advanced Web Tools displays a port name, if there are characters beyond printable ASCII characters (which would have been created by the Host Program), those characters are displayed as dots.

When initially installed, a switch allows any port to dynamically communicate with any other port. Two connectivity attributes are defined to restrict this any-to-any capability for external ports: *Block* and *Prohibit*.

Block is a port connectivity attribute that prevents all communication through a port. Prohibit is the port connectivity attribute that prohibits or allows dynamic communication between ports when a port is not blocked. Each port has a vector specifying its Prohibit attribute with respect to each of the other ports in the switch. This attribute is always set symmetrically in that a pair of ports is either prohibited or allowed to communicate dynamically.

The Port Connectivity table (shown in Figure 45 on page 119) displays the Port number (in physical-location format), Port Name (port address name), Block attribute, Prohibit attribute, and Area ID (port address, displayed in hexadecimal) in fixed columns. The right side is a port matrix, which lists all ports by Area ID and identifies prohibited ports. Those columns are scrollable and swappable.

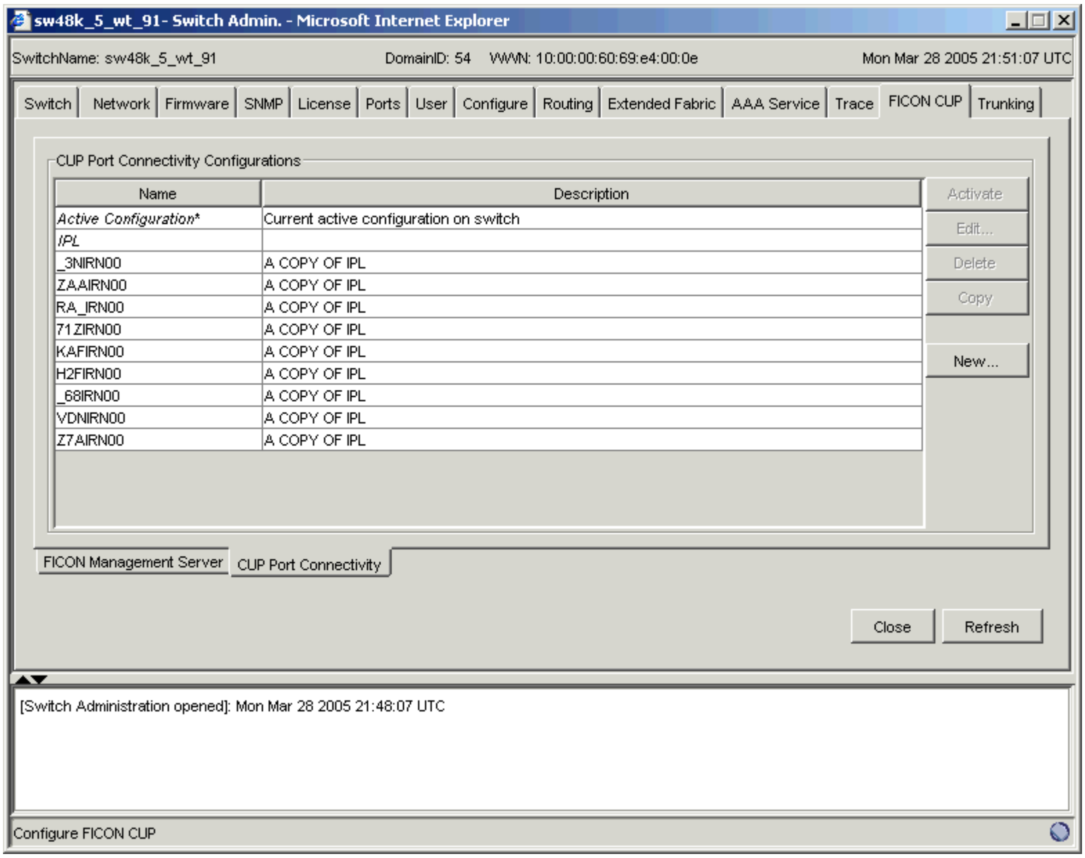
Displaying CUP port connectivity configurations

Use the following procedure to display a list of CUP port connectivity configurations, as shown in Figure 44.

Displaying the CUP port connectivity configurations list

1. Click a FICON-enabled switch from the Fabric Tree.
2. Launch the Switch Admin module as described on page 36.
3. Click the **FICON CUP** tab.

   The FICON CUP tabbed page is displayed, with the FMS subtabbed page in front (see Figure 42 on page 114). All attributes on this page are read-only until FMS mode is enabled.
4. Click the **CUP Port Connectivity** subtab (see Figure 44).



SwitchName: sw48k_5_wt_91 DomainID: 54 WWN: 10:00:00:60:69:e4:00:0e Mon Mar 28 2005 21:51:07 UTC

CUP Port Connectivity Configurations

Name	Description
*Active Configuration**	Current active configuration on switch
IPL	
_3NIRN00	A COPY OF IPL
ZAAIRN00	A COPY OF IPL
RA_IRN00	A COPY OF IPL
71ZIRN00	A COPY OF IPL
KAFIRN00	A COPY OF IPL
H2FIRN00	A COPY OF IPL
_68IRN00	A COPY OF IPL
VDNIRN00	A COPY OF IPL
Z7AIRN00	A COPY OF IPL

[Switch Administration opened]: Mon Mar 28 2005 21:48:07 UTC

Configure FICON CUP

Figure 44 Configuring CUP port connectivity

Creating or editing CUP port connectivity configurations

Use the following procedure to create a new CUP port connectivity configuration or to edit an existing configuration.

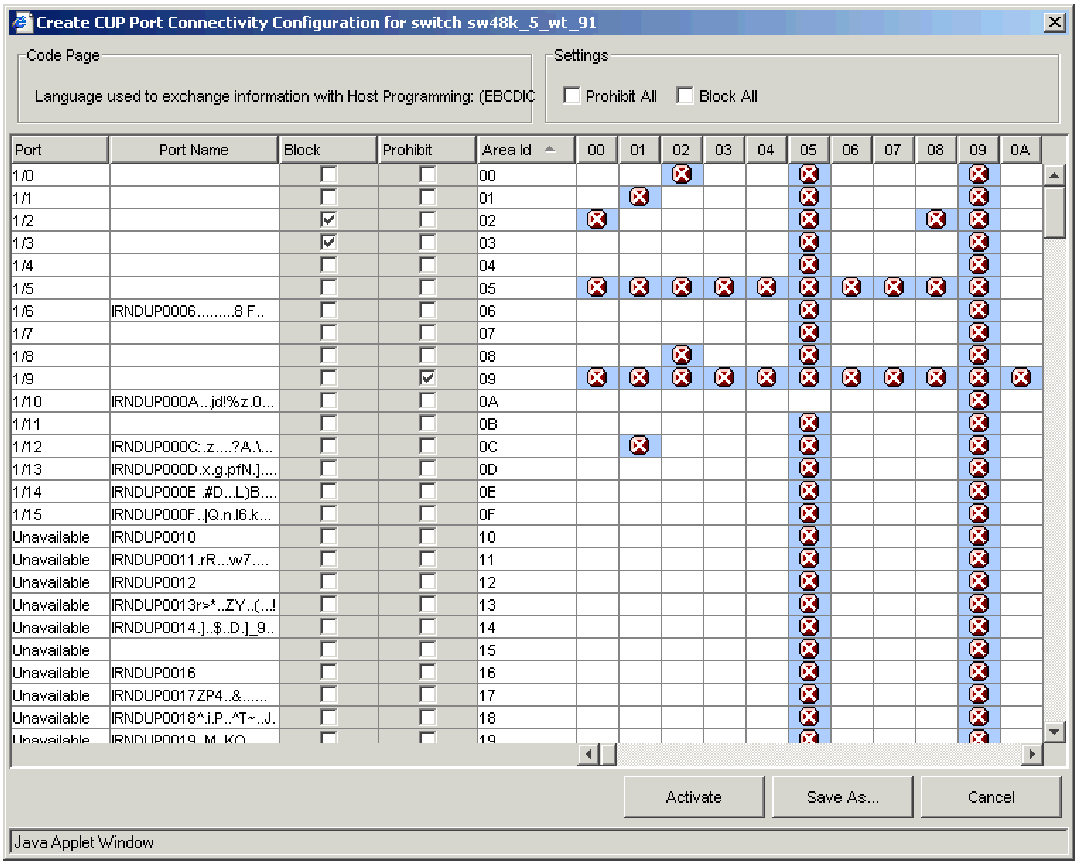
1. Display the CUP port connectivity configuration list, as described on page 117.
2. Create a new configuration or edit an existing configuration:
   - To create a new configuration, click **New**.

     The Create Port CUP Connectivity Configuration dialog box displays all ports and port names on the selected switch (similar to the dialog box shown in Figure 45. The Block column, Prohibit column, and prohibited ports matrix are displayed as empty, for you to configure.
   - To edit an existing configuration, click the configuration and then click **Edit**.

     The Edit Port CUP Connectivity Configuration dialog box displays the content of the selected configuration from the switch in a table format (see Figure 45).
3. Optional: Select the check box corresponding to a port you want to block on the Block column. Repeat this step for all ports you want to block. Select the **Block All** check box to block all ports.
4. Optional: Select the check box corresponding to a port you want to prohibit on the Prohibit column. Repeat this step for all ports you want to prohibit. Select the **Prohibit All** checkbox to prohibit all ports.

   The cells in the matrix are updated with X icons to identify prohibited ports.

5. Optional: Click the individual cells corresponding to the combination of ports you want to prohibit. You cannot prohibit a port to itself.
6. Review your changes. A blue background in a cell indicates that its value has been modified.
7. After you have finished making changes, do any of the following:
    - Click **Activate** to save the changes and make the configuration active immediately, as described in "Port CUP Connectivity Configuration dialog box" on page 119.
    - Click **Save** to save the changes but not make the configuration active.
    - Click **Save As** to save the configuration to a new configuration file. When you click Save As, a dialog box opens in which you enter a file name and description for the configuration file.
    - Click **Refresh** to refresh the information from the switch.
    - Click **Cancel** to cancel all changes without saving.



Create CUP Port Connectivity Configuration for switch sw48k_5_wt_91

Code Page

Language used to exchange information with Host Programming: (EBCDIC

Settings

□ Prohibit All □ Block All

Port	Port Name	Block	Prohibit	Area Id	00	01	02	03	04	05	06	07	08	09	0A
1/0		□	□	00			☒			☒				☒	
1/1		□	□	01		☒				☒				☒	
1/2		☑	□	02	☒					☒			☒	☒	
1/3		☑	□	03						☒				☒	
1/4		□	□	04						☒				☒	
1/5		□	□	05	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	
1/6	IRNDUP0006.........8 F..	□	□	06						☒				☒	
1/7		□	□	07						☒				☒	
1/8		□	□	08			☒			☒				☒	
1/9		□	☑	09	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
1/10	IRNDUP000A...jd!%z.0...	□	□	0A										☒	
1/11		□	□	0B						☒				☒	
1/12	IRNDUP000C:.z....?A.\...	□	□	0C		☒				☒				☒	
1/13	IRNDUP000D.x.g.pfN.]....	□	□	0D						☒				☒	
1/14	IRNDUP000E .#D...L)B....	□	□	0E						☒				☒	
1/15	IRNDUP000F..|Q.n.l6.k...	□	□	0F						☒				☒	
Unavailable	IRNDUP0010	□	□	10						☒				☒	
Unavailable	IRNDUP0011.rR...w7....	□	□	11						☒				☒	
Unavailable	IRNDUP0012	□	□	12						☒				☒	
Unavailable	IRNDUP0013r>*..ZY..(...!	□	□	13						☒				☒	
Unavailable	IRNDUP0014.]..$..D.]_9..	□	□	14						☒				☒	
Unavailable		□	□	15						☒				☒	
Unavailable	IRNDUP0016	□	□	16						☒				☒	
Unavailable	IRNDUP0017ZP4..&......	□	□	17						☒				☒	
Unavailable	IRNDUP0018^.i.P..^T~..J.	□	□	18						☒				☒	
Unavailable	IRNDUP0019..M..KQ	□	□	19						☒				☒	

Figure 45 Port CUP Connectivity Configuration dialog box

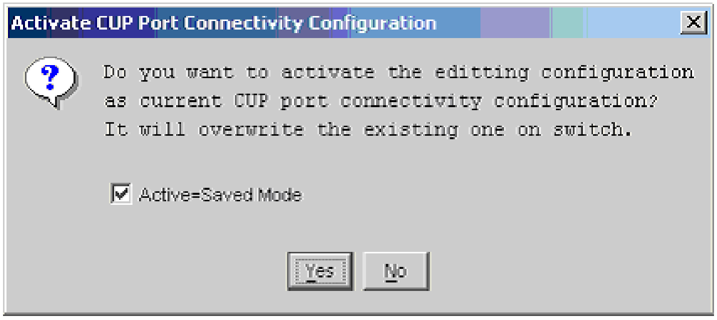
Activating a CUP port connectivity configuration

When you activate a saved CUP port connectivity configuration on the switch, the preceding configuration (currently activated) is overwritten.

Activating a saved CUP port connectivity configuration

1. Display the CUP port connectivity configuration list, as described on page 117.
2. Click the saved configuration from the list.
3. Click **Activate**.

The Activate CUP Port Connectivity Configuration confirmation dialog box opens (Figure 46).



Activate CUP Port Connectivity Configuration

Do you want to activate the editting configuration as current CUP port connectivity configuration? It will overwrite the existing one on switch.

☑ Active=Saved Mode

Figure 46 Activate CUP Port Connectivity configuration dialog box

The dialog box reminds you that the current configuration is overwritten upon activation.

4. Optional: Select **Active=Saved Mode** to enable (checked) or disable (unchecked) the Active=Saved FMS parameter after the configuration is activated.
5. Click **Yes** to activate the configuration, or click **No** to cancel the activation.

Copying a CUP port connectivity configuration

Use the following procedure to copy a CUP port connectivity configuration to a new configuration.

1. Display the CUP port connectivity configuration list, as described on page 117.
2. Click a saved configuration or the active configuration from the list.
3. Click **Copy**.

   The Copy CUP Port Connectivity Configuration dialog box opens.
4. In the dialog box, enter a name and description for the new configuration and click **OK** to save the configuration to the target file; click **Cancel** to cancel copying the configuration.

   The file name must be in alphanumeric characters and can contain only dashes or underscores as special characters.

Deleting a CUP port connectivity configuration

Use the following procedure to delete a saved CUP port connectivity configuration.

Deleting a saved CUP port connectivity configuration

1. Display the CUP port connectivity configuration list, as described on page 117.
2. Click the saved configuration from the list.
3. Click **Delete**.

   The Delete CUP Port Connectivity Configuration confirmation dialog box opens.
4. Click **Yes** to delete the selected configuration; click **No** to cancel the deletion.

12 Administering Fabric Watch

This chapter contains the following sections:

Introduction to Fabric Watch

IMPORTANT: Fabric Watch is an HP optional, licensed feature that monitors the performance and status of switches and can alert you when problems arise, before they become costly failures.

Fabric Watch tracks a variety of SAN fabric elements, events, and counters. For example, Fabric Watch monitors:

- Fabric resources, including fabric reconfigurations, zoning changes, and new logins
- Switch environmental functions, such as temperature, power supply, and fan status, along with security violations
- Port state transitions, errors, and traffic information for multiple port classes as well as operational values for supported models of Finisar Smart GBICs/SFPs
- Performance information for AL_PA, end-to-end (EE), and SCSI command metrics

Fabric Watch lets you define how often to measure each switch and fabric element and allows you to specify notification thresholds. Whenever fabric elements exceed these thresholds, Fabric Watch provides notification using several methods, including e-mail messages, SNMP traps, and log entries.

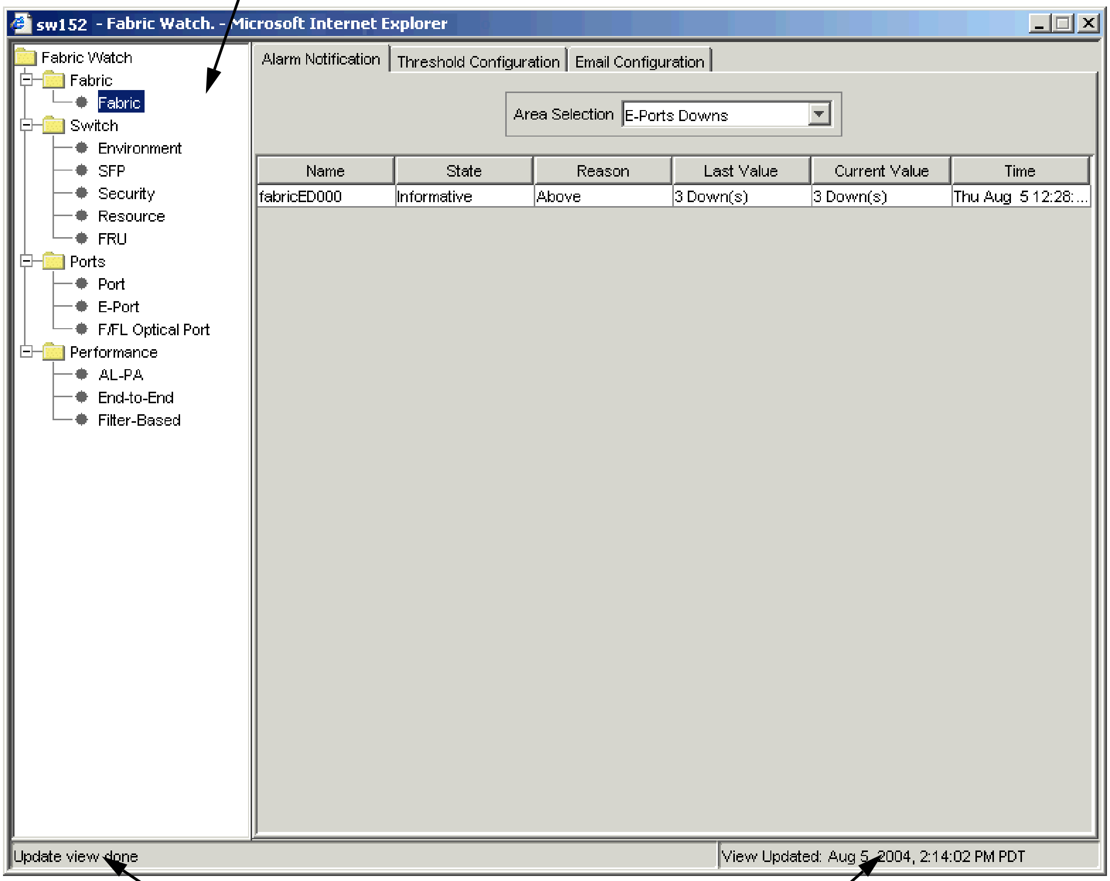
NOTE: To use the Fabric Watch feature, you must have a Fabric Watch license installed on your switch.

For more detailed information regarding Fabric Watch, see the *HP StorageWorks Fabric OS 5.x Fabric Watch administrator guide*.

Using Fabric Watch with Advanced Web Tools

You can administer Fabric Watch operations through the Advanced Web Tools Fabric Watch module. To access the Fabric Watch module, shown in Figure 47, click the Watch button in the Switch View

Fabric Watch navigation tree, lists the available classes for the switch



Area Selection: E-Ports Downs

Name	State	Reason	Last Value	Current Value	Time
fabricED000	Informative	Above	3 Down(s)	3 Down(s)	Thu Aug 5 12:28:...

Update view done

View Updated: Aug 5, 2004, 2:14:02 PM PDT

Summary of actions

The last time the Fabric Watch module was updated

Figure 47 Fabric Watch module

The Fabric Watch navigation tree, on the left side of the module, displays the available classes. The classes are organized in a set of folders. Not all classes are available for all switches.

You should use the Fabric Watch module if you want to:

- Configure custom threshold values on particular elements.
- Place limits on the acceptable values of those elements and enable the custom limits (configure threshold boundaries).
- Choose if and how Fabric Watch alerts you to errant values (configure alarms).
- Choose if and how frequently Fabric Watch identifies unacceptable values (configure threshold traits).

Launching the Fabric Watch module

1. Select a switch from the Fabric Tree.

   The selected switch appears in the Switch View.
2. Click the **Watch** button on the Switch View.

NOTE: The Watch button is displayed in the Switch View only if the Fabric Watch license has been activated.

The Fabric Watch module is displayed (see Figure 47).

Configuring Fabric Watch thresholds

The Threshold Configuration tab enables you to configure event conditions. From this tab, you configure threshold traits, alarms, and e-mail configuration.

Use the following procedures to configure threshold traits for all classes except for the FRU class. Use the procedure described in "Configuring alarms for FRUs" on page 125 for the FRU class.

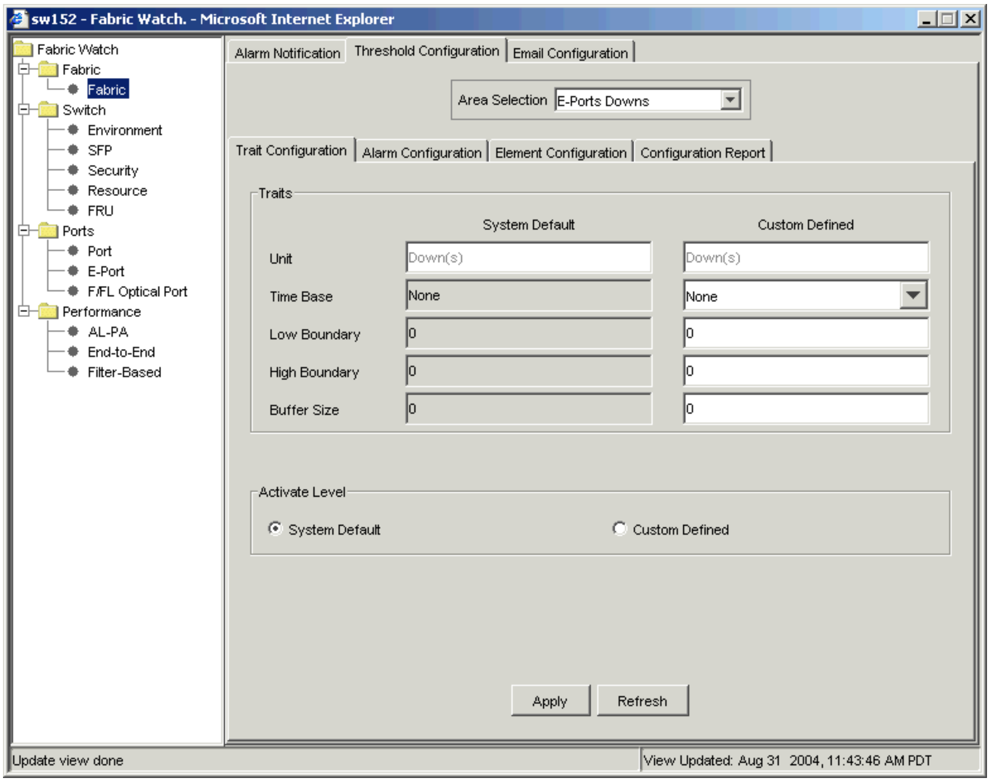
Configuring threshold traits

Configure threshold traits to define a threshold for a particular class and area. Using the following procedure, you can configure the following traits for a threshold:

- Unit: The string used to define the units of measurement for the area
- Time Base: The time base (second, minute, hour, day) for the area
- Low Boundary: The low threshold for the event-setting comparisons
- High Boundary: The high threshold for the event-setting comparisons
- Buffer Size: The size of the buffer zone used in event-setting comparisons

To configure threshold traits

1. Launch the Fabric Watch module as described in "Launching the Fabric Watch module" on page 122.
2. Click the **Threshold Configuration** tab (see Figure 48).



Area Selection: E-Ports Downs

Traits

	System Default	Custom Defined
Unit	Down(s)	Down(s)
Time Base	None	None
Low Boundary	0	0
High Boundary	0	0
Buffer Size	0	0

Activate Level

● System Default ○ Custom Defined

Update view done

View Updated: Aug 31 2004, 11:43:46 AM PDT

Figure 48 Threshold configuration for Fabric Watch

3. Click the **Trait Configuration** subtab.
4. Click a class from the Fabric Watch navigation tree.

NOTE: If you select the FRU class from the Fabric Watch navigation tree, there is a separate set of instructions. See "Configuring alarms for FRUs" on page 125.

5. Select an area from the Area Selection menu in the Threshold Configuration tabbed page.

   The module displays two columns of trait information, labeled System Default and Custom Defined. You cannot modify the information in the System Default column.
6. Select the **System Default** radio button to use the system default settings, and go to step 12, or select the **Custom Defined** radio button to specify new settings and continue with the next step.
7. Enter a unit of threshold measurement in the Unit box.
8. Select a time to record the event in the Time Base box.
9. Enter the lowest boundary of the normal zone in the Low Boundary box.
10. Enter the highest boundary of the normal zone in the High Boundary box.
11. Enter the size of the buffer zone in the Buffer Size box.
12. Click **Apply** to save your changes.

Configuring threshold alarms

After you update the threshold information, use the Alarm Configuration subtab to customize the notification settings for each event setting.

1. Launch the Fabric Watch module as described on page 122.
2. Select the **Threshold Configuration** tab.
3. Select the **Alarm Configuration** subtab.
4. Click a class from the Fabric Watch navigation tree.
5. Select an area from the Area Selection menu in the Threshold Configuration tab.

   The module displays two tables of alarm configuration information, labeled System Default and Custom Defined. You cannot modify the information in the System Default table.
6. Select the **System Default** radio button in the Activate Level section to use the system default settings, and proceed to step 8, or select the **Custom Defined** radio button in the Activate Level section to specify new settings, and then proceed to the next step.
7. Select a check box to set the type of notification method for each event type (Changed, Below, Above, Inbetween).

   The available alarm actions are ERROR_LOG, SNMP_TRAP, RAPI_TRAP, and EMAIL_ALERT.
8. Click **Apply**.

Enabling or disabling threshold alarms for individual elements

Use the Element Configuration subtab to configure element-specific alarm settings.

Enabling or disabling threshold alarms for an element

1. Launch the Fabric Watch module as described on page 122.
2. Click a class from the Fabric Watch navigation tree.

   You can set alarms for information on a switch only if that information is monitored by Fabric Watch for that switch; not all alarm options are available for all switches. For more information, see the *HP StorageWorks Fabric OS 5.x Fabric Watch administrator guide*.
3. Click the **Threshold Configuration** tab.
4. Click the area with the alarms that you want to enable or disable from the Area Selection menu.
5. Click the **Element Configuration** subtab.
6. Click an element from the Element Selection menu.
7. To disable threshold alarms, click **Disabled** in the Status area, and then click **Apply** (the threshold alarms are disabled and you do not need to continue with this procedure).

   To enable threshold alarms, click **Enabled** in the Status area, and continue with the next step.

8. Select a behavior type for the threshold alarms:
   - Click **Triggered** to receive threshold alarms only when they are triggered by events that you have defined.
   - Click **Continuous** to receive threshold alarms at a continuous interval. Select a time interval in which to receive the threshold alarms from the Time Interval menu.
9. Click **Apply**.
10. Optional: Apply the selections on this panel to multiple elements simultaneously:
    a. Click **Apply More**.

       This opens the Multiple Selection dialog box.

    b. Click the boxes next to the indices of all applicable elements.

    c. Click **OK**.

Configuring alarms for FRUs

Configuration for the FRU class is different than configuration for the other classes. Because FRUs are not monitored through a threshold-based system, they have a simpler interface for configuration. For FRUs, you configure the states for which an event occurs, as described in the following procedure.

1. Launch the Fabric Watch module as described on page 122.
2. Click the **Threshold Configuration** tab.
3. Click the FRU class from the Fabric Watch navigation tree.
4. Select a FRU type from the Area Selection menu in the Threshold Configuration tab.
5. Click the alarm states for which you want an event to register.

   Whenever a FRU of the selected type is detected to be in one of the selected states, an event occurs.
6. Click the methods by which you want to be notified about the FRU alarms.

   For FRUs, the only options are error log and e-mail alert.
7. Click **Apply** to apply the changes to the switch.

   A confirmation dialog box opens, asking whether you want to apply the changes to the switch.
8. Click **OK** in the confirmation dialog box to save the changes to the switch.

Displaying Fabric Watch alarm information

From the Fabric Watch module, you can view two types of reports:

- Alarm notifications, which displays the alarms that have occurred for a selected class/area
- Alarm configuration, which displays threshold and alarm configurations for a selected class/area

Displaying an alarm configuration report

Use the Threshold Configuration tab, Configuration Report subtab to display a report of the configuration for a selected class/area. The following information is displayed:

- Threshold settings (labeled Threshold Configuration)
- Notification settings (labeled Action Configuration)
- Element settings (not labeled)

You can scroll through this information but cannot make changes.

Viewing an alarm configuration report

1. Launch the Fabric Watch module as described on page 122.
2. Select the **Threshold Configuration** tab.
3. Click a previously configured element from the Fabric Watch navigation tree (see "Enabling or disabling threshold alarms for individual elements" on page 124).
4. Select the alarm area report to be viewed from the Area Selection menu.
5. Select the **Configuration Report** subtab.

   This tab displays a report of the configuration for the selected area.

Displaying alarms

Using the Alarm Notification tab, you can view a list of all alarms that have occurred for a selected class/area (see Figure 47 on page 122). Table 11 describes the columns in this report.

NOTE: For the FRU class, only the Name, State, and Time columns are displayed. In addition, if the FRU area is Fan, the Name column refers to either a fan or a fan FRU, depending on the switch model. See "Displaying detailed fan hardware status" on page 106 for more information.

Table 11 Alarm notification table fields

Field	Description
Name	The string assigned to the element that had an event
State	The current state of the element
Reason	The event type that was triggered
Last Value	The data value of the element when the event was triggered
Current Value	The current data value of the element
Time	Time when the event occurred

Viewing alarms

1. Launch the Fabric Watch module as described on page 122.
2. Click the class that you want to check for alarms in the Fabric Watch navigation tree.
3. Click the **Alarm Notification** tab.
4. Click the area that you want to check for alarms from the Area Selection menu.

   All alarms for that area are displayed.

For troubleshooting responses to alarms, see the *HP StorageWorks Fabric OS 5.x Fabric Watch administrator guide*.

Configuring e-mail notifications

One of the ways that you can be notified of an alarm condition is through an e-mail alert. If you have configured alarms to send an e-mail notification, you must also configure the e-mail server and the e-mail recipient, as described in the following sections.

Configuring the e-mail server on a switch

You must set up the e-mail notification recipient's DNS server and domain name on each switch for which e-mail notification is enabled.

When you set up the e-mail notification local network's DNS server and domain name for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, the set-up is on a logical-switch basis. This means that for each logical switch, you must set up the e-mail notification recipient's DNS server and domain name individually.

Configuring the e-mail server

1. Launch the Switch Admin module as described on page 36.
2. Select the **Switch** tab.
3. Enter your primary domain Name Server IP address in the DNS Server 1 box in the Email Configuration area.
4. Enter your secondary domain server IP address in the DNS Server 2 box.
5. Enter the domain name (between 4 and 32 characters) in the Domain Name box.
6. Click **Apply** to save the changes.

Configuring the e-mail alert recipient

You can set a different e-mail alert configuration for each class. For example, you can set one e-mail notification for SFPs and another for E_Ports. Before configuring e-mail alert recipients, you must set up the e-mail notification recipient's DNS server and domain name. For more information, see "Configuring the e-mail server on a switch" on page 126.

Configuring the e-mail alert alarm

1. Launch the Fabric Watch module as described on page 122.
2. Select the **Email Configuration** tab, as shown in Figure 49.
3. Select the **Enable** or **Disable** radio button to enable or disable the e-mail alert status.

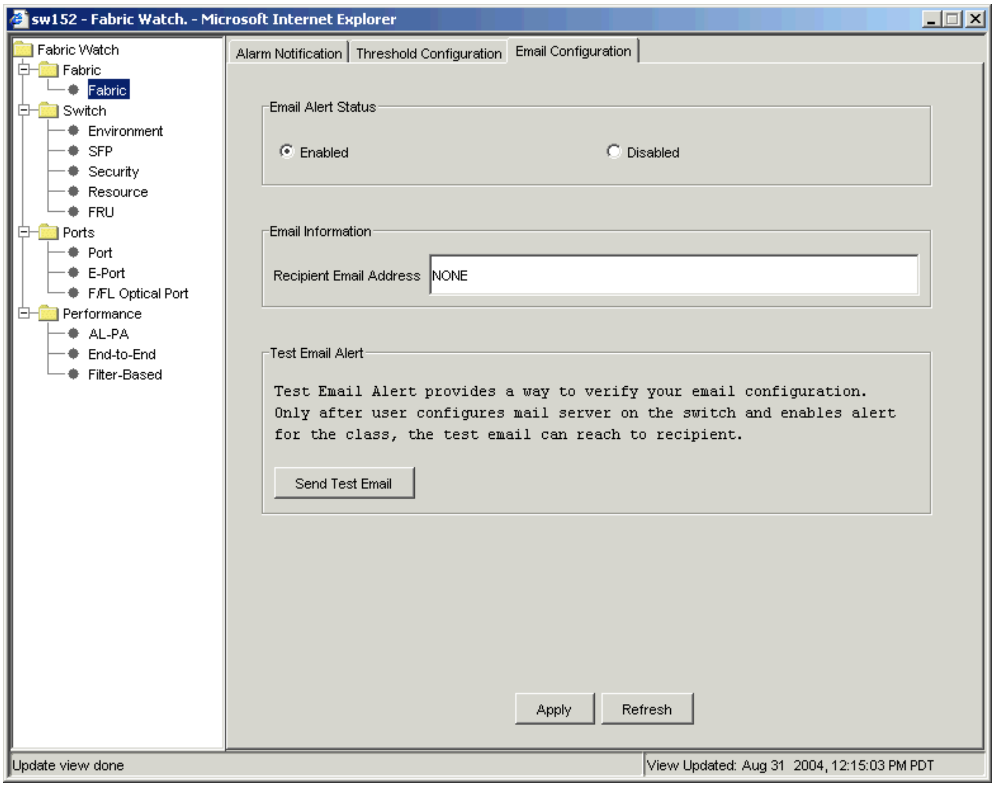
   When you disable e-mail alerts, Fabric Watch does not send e-mail notification even if the e-mail notification method is assigned to monitored areas.
4. Enter the e-mail address of the recipient in the Recipient Email Address text box.

   Messages are sent to this address when e-mail notification is enabled.

NOTE: E-mail addresses must not exceed 128 characters.

5. Click **Apply**.
6. Optional: Click **Send Test Email** to receive a test e-mail so you can verify the e-mail notification is working correctly.

   You can send a test e-mail only after you have applied your settings.



sw152 - Fabric Watch. - Microsoft Internet Explorer

Email Alert Status

● Enabled ○ Disabled

Email Information

Recipient Email Address: NONE

Test Email Alert

Test Email Alert provides a way to verify your email configuration. Only after user configures mail server on the switch and enables alert for the class, the test email can reach to recipient.

Update view done

View Updated: Aug 31 2004, 12:15:03 PM PDT

Figure 49 Fabric Watch e-mail configuration

13 Monitoring performance

This chapter contains the following sections:

Monitoring performance using Advanced Web Tools

The Advanced Web Tools Performance Monitor module graphically displays throughput (in megabytes per second) for each port and for the entire switch.

IMPORTANT: The basic-mode Performance Monitor is standard in the Advanced Web Tools software. The Advanced Monitoring menu in Performance Monitor is optional licensed software.

Use the basic-mode Performance Monitor module to:

- Create user-definable reports.
- Display a performance canvas for application-level or fabric-level views.
- Save persistent graphs across reboots (saves parameter data across reboots).

Using HP Advanced Performance Monitoring, you can display predefined reports for AL_PA, EE, and filter-based performance monitoring. You can track:

- The number of CRC errors for AL_PA devices
- The number of words received and transmitted in Fibre Channel frames with a defined source ID/destination ID (S_ID/D_ID) pair
- The number of times a particular filter pattern in a frame is transmitted by a port

For detailed information on these types of performance monitoring, see the *HP StorageWorks Fabric OS 5.x administrator guide*.

Each graph is displayed individually in a window, so it can be minimized, maximized, resized, and closed.

Graphs within the Performance Monitor module are updated every 30 seconds. When you first display the graph, or if you modify the graph (to add additional ports, for example), you might have to wait up to 30 seconds before the new values appear.

When you have multiple graphs open in the Performance Monitor module, you can:

- Select Tile from the Window menu to view all graphs at once, tiled in the Performance Monitor module.
- Select Cascade from the Window menu to view one graph at a time.
- Select Close All to close all open Performance Monitor graphs in the Performance Monitor module.

In addition, the Window menu lists all open graphs. You can select a graph name from the Window menu to bring that graph to the front view when the graphs are cascaded, and to select the window for that graph when the graphs are tiled.

Predefined performance graphs

Advanced Web Tools predefines basic graph types, to simplify performance monitoring. A wide range of EE fabric, LUN, device, and port metrics graphs are included. Table 12 lists the basic monitoring graphs available. Table 13 lists the advanced monitoring graphs. The advanced monitoring graphs give more detailed performance information to help you manage your fabric. You can access the basic monitoring graphs on all switches; advanced monitoring graphs are available only on switches that have an HP Advanced Performance Monitoring license activated.

Table 12 Basic performance graphs

Graph type	Description
Port Throughput	Displays the performance of a port, in bytes per second, for frames received and transmitted.
Switch Aggregate Throughput	Displays the aggregate performance of all ports on a switch.
Blade Aggregate Throughput	Displays the aggregate performance of all ports on a port card. This graph is available only for the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director.
Switch Throughput Utilization	Displays the port throughput at the time the sample is taken. For the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, this graph displays the throughput for each slot. You can customize this graph to display information for particular ports.
Port Error	Displays a line of CRC errors for a given port.
Switch Percent Utilization	Displays the percentage utilization for each port in a switch. For the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, this graph displays the percent utilization for each slot. You can customize this graph to display information for particular ports.
Port Snapshot Error	Displays the CRC error count between sampling periods for all the ports on a switch. For the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, this graph displays the CRC error rate for each slot. You can customize this graph to display information for particular ports.

Table 13 Advanced performance monitoring graphs

Graph type	Description
SID/DID Performance	Displays the traffic between the SID-DID pair on the switch being managed. For more information, see "Creating an SID/DID performance graph" on page 134.
SCSI vs. IP Traffic	Displays percentage of SCSI versus IP frame traffic on each individual port. For more information, see Creating a SCSI vs. IP traffic graph, page 136.
AL_PA Errors	Displays CRC errors for a given port and a given AL_PA. For more information, see Creating an AL_PA error graph, page 137.
SCSI Commands by port and LUN (R, W, R/W)	Displays the total number of read/write commands on a given port to a specific LUN. For more information, see Creating a SCSI command graph, page 136.

The labeling of axes in the graphs depends on the switch type. For the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, slot numbers are displayed with expansion arrows next to them. Click the arrows to expand and contract the list of ports per slot. For the 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, 4Gb SAN Switch for HP p-Class BladeSystem, and SAN Switch 4/32, slot numbers are not identified.

Figure 50 shows how to access the list of Advanced Performance Monitoring graphs using Advanced Web Tools. This example displays the graphs available in the Performance Monitor module for a SAN Director 2/128 with the Advanced Performance Monitoring license installed. Note that the slot number is identified.

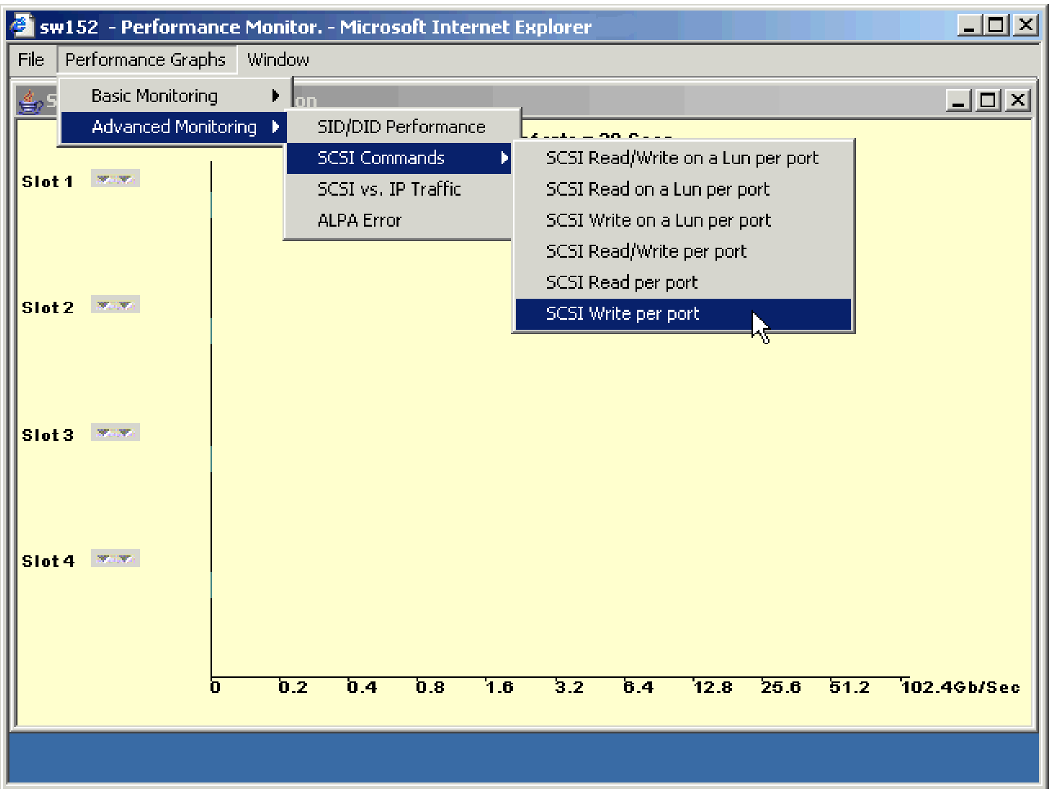


Figure 50 Accessing performance graphs

User-defined graphs

You can modify the predefined graphs to create your own customized graphs (see "Customizing basic Performance Monitor graphs" on page 133 for more information). These user-defined graphs can be added and saved to canvas configurations, described next.

Canvas configurations

A *canvas* is a saved configuration of graphs. The graphs can be either the Advanced Web Tools predefined graphs or user-defined graphs. Each canvas can hold up to eight graphs per window, as shown in Figure 51. Up to 20 canvases can be set up for different users or different scenarios. Each canvas is saved with a name and an optional brief description.

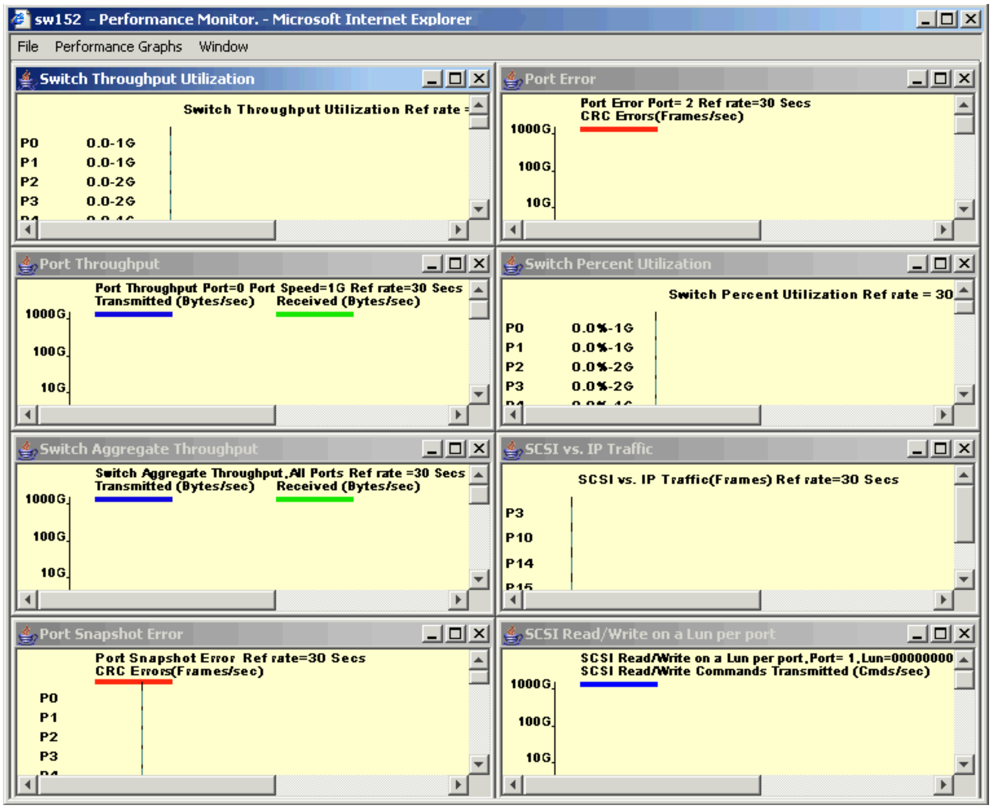

sw152 - Performance Monitor. - Microsoft Internet Explorer
File
Performance Graphs
Window
Switch Throughput Utilization
Switch Throughput Utilization Ref rate =
P0 0.0-1G
P1 0.0-1G
P2 0.0-2G
P3 0.0-2G
Port Error
Port Error Port= 2 Ref rate=30 Secs
CRC Errors(Frames/sec)
1000G
100G
10G
Port Throughput
Port Throughput Port=0 Port Speed=1G Ref rate=30 Secs
Transmitted (Bytes/sec)
Received (Bytes/sec)
1000G
100G
10G
Switch Percent Utilization
Switch Percent Utilization Ref rate = 30
P0 0.0%-1G
P1 0.0%-1G
P2 0.0%-2G
P3 0.0%-2G
Switch Aggregate Throughput
Switch Aggregate Throughput,All Ports Ref rate =30 Secs
Transmitted (Bytes/sec)
Received (Bytes/sec)
1000G
100G
10G
SCSI vs. IP Traffic
SCSI vs. IP Traffic(Frames) Ref rate=30 Secs
P3
P10
P14
Port Snapshot Error
Port Snapshot Error Ref rate=30 Secs
CRC Errors(Frames/sec)
P0
P1
P2
P3
SCSI Read/Write on a Lun per port
SCSI Read/Write on a Lun per port,Port= 1,Lun=00000000
SCSI Read/Write Commands Transmitted (Cmds/sec)
1000G
100G
10G

Figure 51 Canvas of eight performance monitoring graphs

Launching the Performance Monitor module

Use the following procedure to launch the Advanced Web Tools Performance Monitor module.

1. Select a switch from the Fabric Tree.

   The selected switch appears in the Switch View.

2. Click the **Perf** button on the Switch View.

   The Performance Monitor module is displayed.

Creating a basic Performance Monitor graph

Use the following procedure to create the basic Performance Monitor graphs listed in Table 12 on page 130.

1. Launch the Performance Monitor module as described on page 132.
2. Select **Performance Graphs > Basic Monitoring >** ***Graph Type***.

   Depending on the type of graph you select, you might be prompted to select a slot or port for which to create a graph (see Figure 52).

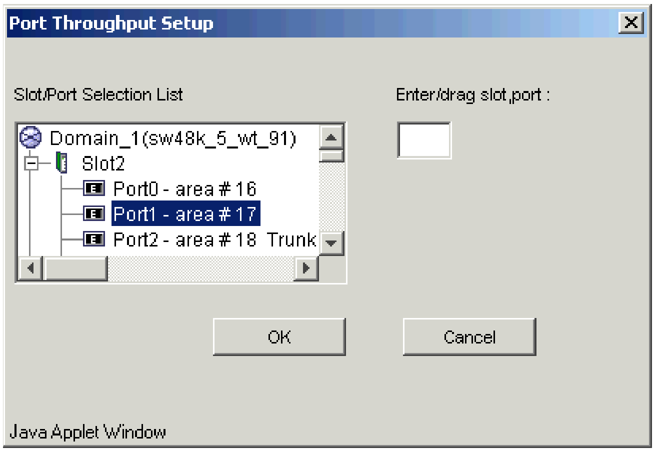


Figure 52 Creating a port throughput graph

3. If prompted, drag the port into the Enter/drag slot,port box, or enter the slot and port information in the box, in the format `slot,port`.
   - For Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, you must select first a slot number and then a port number.
   - For 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, 4Gb SAN Switch for HP p-Class BladeSystem, and SAN Switch 4/32, you need enter only a port number.
4. Click **OK**.

   The graph is displayed in a window in the Performance Monitor module. The next section explains how you can customize some of these graphs.

Customizing basic Performance Monitor graphs

You can customize some of the basic Performance Monitor graphs to display information for particular ports. For the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, you can also customize these graphs to display information for a slot.

You can customize the following graphs:

- Switch Throughput Utilization Graph
- Switch Percent Utilization Graph
- Port Snapshot Error Graph

The following procedure assumes that you have already created one of these customizable graphs.

Customizing a basic Performance Monitor graph

1. Create or access the graph you want to customize.

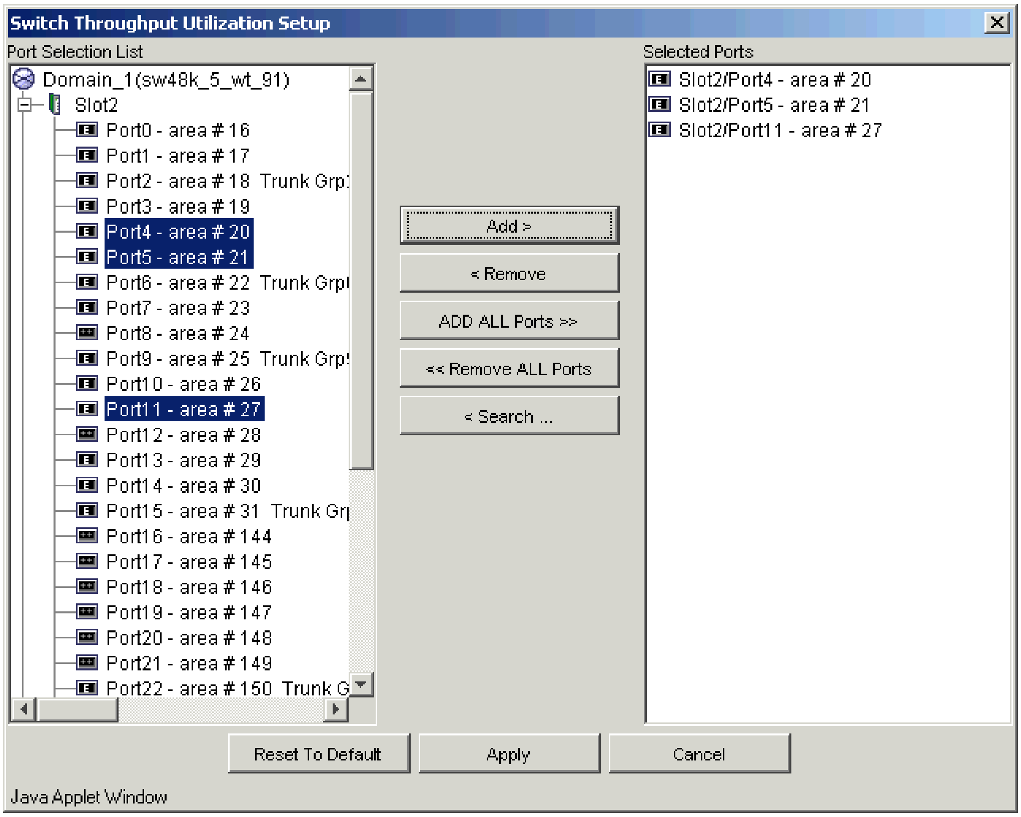
   See "Creating a basic Performance Monitor graph" on page 132 for instructions on creating a graph.
2. For Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, to display detailed port throughput utilization rates for each port in a slot, click the arrows next to a slot. Port information for that slot is displayed in the graph.

   For 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, 4Gb SAN Switch for HP p-Class BladeSystem, and SAN Switch 4/32, proceed to step 3.
3. Display detailed port throughput utilization rates for particular ports only:

   a. Right-click anywhere in the graph.

   b. Click **Select Ports**.

      The setup dialog box opens, as shown in Figure 53. The title of the dialog box varies, depending on the type of graph you are customizing, but the layout of the dialog box is the same. Figure 53 shows an example of the setup dialog box for the Switch Throughput Utilization graph.



Domain_1(sw48k_5_wt_91)
Slot2
Port0 - area # 16
Port1 - area # 17
Port2 - area # 18 Trunk Grp
Port3 - area # 19
Port4 - area # 20
Port5 - area # 21
Port6 - area # 22 Trunk Grp
Port7 - area # 23
Port8 - area # 24
Port9 - area # 25 Trunk Grp
Port10 - area # 26
Port11 - area # 27
Port12 - area # 28
Port13 - area # 29
Port14 - area # 30
Port15 - area # 31 Trunk Gr
Port16 - area # 144
Port17 - area # 145
Port18 - area # 146
Port19 - area # 147
Port20 - area # 148
Port21 - area # 149
Port22 - area # 150 Trunk G

Slot2/Port4 - area # 20
Slot2/Port5 - area # 21
Slot2/Port11 - area # 27

Figure 53 Switch Throughput Utilization Setup dialog box

c. Double-click the domain icon ⊗ to expand the slot/port list.

For the Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, click the **+** signs to expand the ports under each slot, as shown in Figure 53.

d. Click the port you want to monitor in the graph in the Port Selection List. Use **Shift-click** and **Ctrl-click** to select multiple ports.

e. Click **Add** to move the selected ports to the Selected Ports list.

f. Optional: Click **ADD ALL Ports** to add all of the ports in the Port Selection List to the Selected Ports list.

g. Optional: Click **Search** to launch the Search Port Selection List dialog box, from which you can search for all E_Ports, all F_Ports, or all port names with a defined string. Select the ports you want to add and click **Search** in the Search Port Selection List dialog box.

h. Click **Apply**.

Only the selected ports are displayed in the graph.

Creating advanced Performance Monitor graphs

This section describes how to create the advanced Performance Monitor graphs listed in Table 13 on page 130. Because the procedure for creating these graphs differs depending on the type of graph, each type is described separately in the sections that follow.

NOTE: You must have an Advanced Performance Monitor license installed to use the advance Performance Monitor features.

Creating an SID/DID performance graph

The SID/DID performance graph displays the traffic between a SID-DID pair on the switch being managed.

Creating an SID/DID performance graph

1. Launch the Performance Monitor module as described on page 132.
2. Select **Performance Graphs > Advanced Monitoring > SID/DID Performance**.

   The SID/DID Performance Setup dialog box opens (see Figure 54).

   If you want to see which EE monitors are currently set up on a particular port, go to step 3.

   If you want to specify the port, source ID, and domain ID, go to step 4.

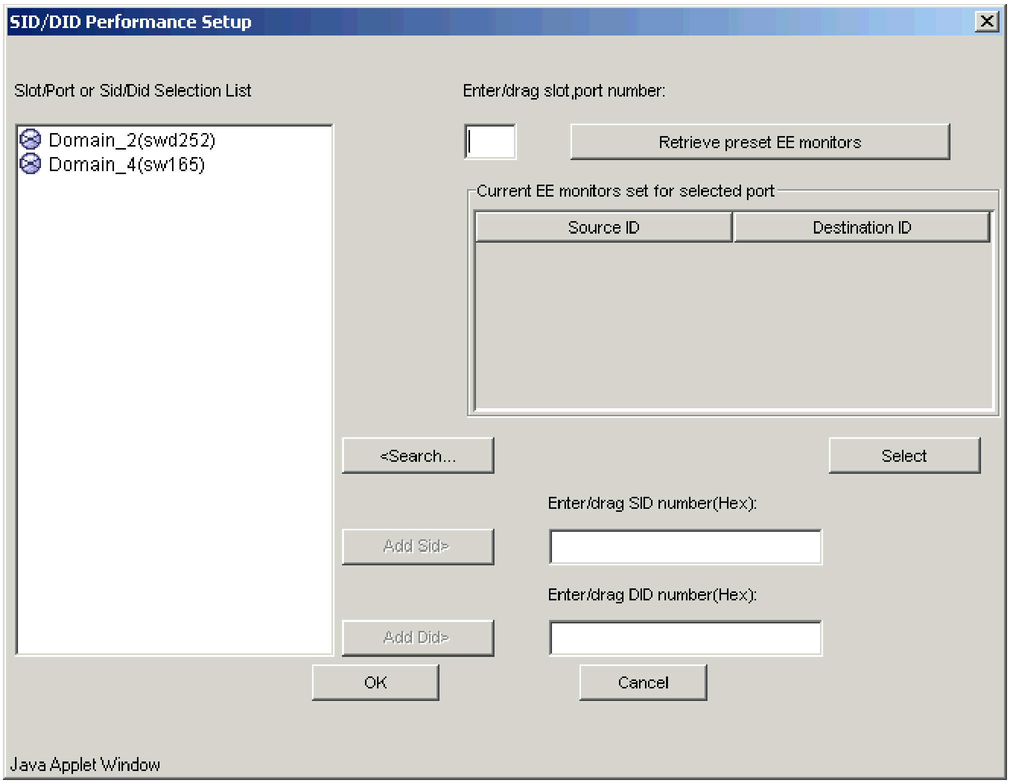

SID/DID Performance Setup
Slot/Port or Sid/Did Selection List
Domain_2(swd252)
Domain_4(sw165)
Enter/drag slot,port number:
Retrieve preset EE monitors
Current EE monitors set for selected port
Source ID
Destination ID
<Search...
Select
Enter/drag SID number(Hex):
Add Sid>
Enter/drag DID number(Hex):
Add Did>
OK
Cancel
Java Applet Window

Figure 54 Creating an SID/DID performance graph

3. Click a port from the Slot/Port or Sid/Did Selection List.
   a. Drag the selected port into the Enter/drag port number box.
   b. Click **Retrieve preset EE monitors**.

      The current EE monitors for that port are displayed in the Current EE monitors set for selected port table.
   c. Optional: To display a performance graph for the current EE monitors set for the selected port, click a SID/DID pair in the table. You can select multiple source ID and Destination IDs. Click **Select**. If you selected multiple SID/DID monitors, click **OK** in the confirmation dialog box that appears. Skip to step 6.

      If you do not want to display a performance graph for the current EE monitors set for the selected port, continue with step 4.
4. Select a source ID from the Port or Sid/Did Selection List, and click **Add Sid**.

   You can also enter a source ID in the Enter/drag SID number box.
5. Select a destination ID from the Port or Sid/Did Selection List, and click **Add Did**.

   You can also enter a destination ID in the Enter/drag DID number box.
6. Click **OK**.

   If you selected multiple EE monitors, SIDs, or PIDs, a confirmation dialog box opens, reminding you that one graph will be opened for each selection. Click **Yes** to display the graphs.

Creating a SCSI vs. IP traffic graph

The SCSI vs. IP Traffic graph displays the SCSI vs. IP traffic for selected ports. For Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, the slot and port name is identified in the graph.

In a trunk group, the SCSI vs. IP Traffic graph displays only the master port, not the slave ports.

To create a SCSI vs. IP traffic graph

1. Launch the Performance Monitor module as described on page 132.
2. Select **Performance Graphs > Advanced Monitoring > SCSI vs. IP Traffic**.

   The SCSI vs. IP Traffic Setup dialog box opens. This dialog box is similar to that shown in Figure 53 on page 134.
3. Double-click the domain icon to expand the slot/port list.

   For Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director, click the **+** signs to expand the ports under each slot, as shown in Figure 53.
4. Click the port you want to monitor in the graph in the Port Selection List. Use **Shift-click** and **Ctrl-click** to select multiple ports.
5. Click **Add** to move the selected ports to the Selected Ports list.
6. Optional: Click **ADD ALL Ports** to add all of the ports in the Port Selection List to the Selected Ports list.
7. Optional: Click **Search** to launch the Search Port Selection List dialog box, from which you can search for all E_Ports, all F_Ports, or all port names with a defined string. Select the ports you want to add and click **Search** in the Search Port Selection List dialog box.
8. Click **Apply** in the SCSI vs. IP Traffic Setup dialog box.

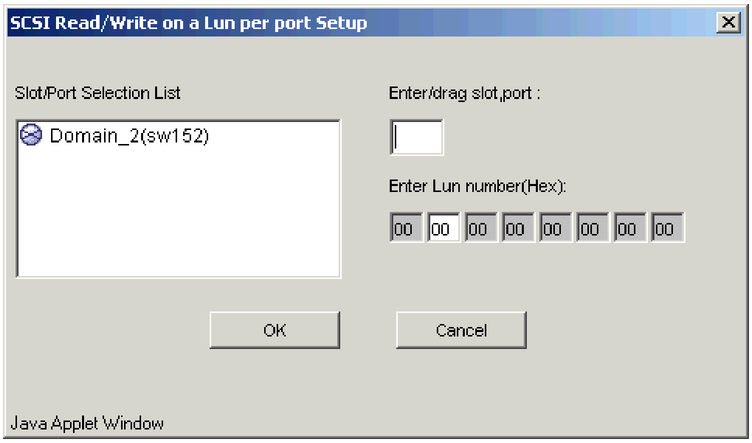
   Only the selected ports are displayed in the SCSI vs. IP traffic graph.

Creating a SCSI command graph

This graph displays the total number of read or write (or both) commands on a given port or to a specific LUN on a given port.

1. Launch the Performance Monitor module as described on page 132.
2. Select **Performance Graphs > Advanced Monitoring > SCSI Commands >** ***Graph Type***.

   The applicable setup dialog box opens. Figure 55 shows the SCSI Read/Write on a LUN per port Setup dialog box.



SCSI Read/Write on a Lun per port Setup

Slot/Port Selection List

Domain_2(sw152)

Enter/drag slot,port :

Enter Lun number(Hex):

00 00 00 00 00 00 00 00

Figure 55 Creating a SCSI command graph

3. Navigate to a ***switch > slot > port*** in the Slot/Port Selection List.
4. Click the port from the Slot/Port Selection List and drag it into the Enter/*drag slot,port* box.

5. Optional: For the LUN per port graphs, enter a LUN number, in hexadecimal:
   - For the 4Gb SAN Switch for HP p-Class BladeSystem and SAN Switch 4/32, you can enter up to eight LUN masks.
   - For the 4/256 SAN Director, you can enter up to four LUN masks.
   - For all other switches running Fabric OS 4.x or 5.x, you can enter up to two LUN masks.
   - For switches running Fabric OS 3.x, you can enter up to three LUN masks.
6. Click **OK**.

   The selected graph is displayed in the canvas.

Creating an AL_PA error graph

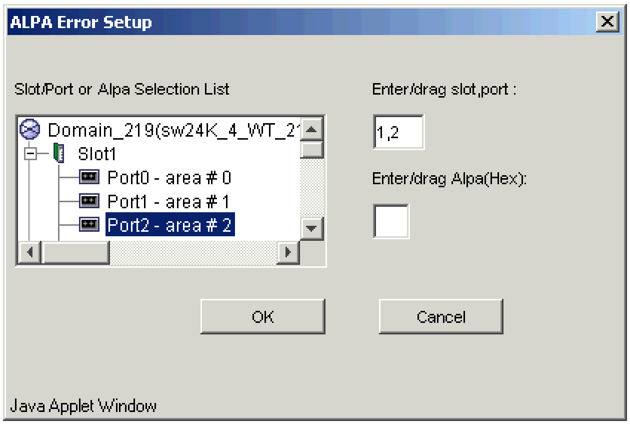
The AL_PA Error graph displays CRC errors for a given port and a given AL_PA. The AL_PA Error graph is not supported on the 4Gb SAN Switch for HP p-Class BladeSystem and SAN Switch 4/32.

1. Launch the Performance Monitor module as described on page 132.
2. Select **Performance Graphs > Advanced Monitoring > ALPA Error**.

   The ALPA Error Setup dialog box opens (see Figure 56).
3. Navigate to a ***switch > slot > port*** in the Slot/Port or Alpa Selection List.
4. Click the port or Alpha from the Slot/Port or Alpha Selection List or an AL_PA from the Slot/Port Selection List, and drag it into the Enter/*drag slot,port* box.

   You can also enter the slot and port number in the format `slot,port`.
5. Click **OK**.

   The AL_PA error graph is displayed on the canvas.



Enter/drag slot,port : 1,2

Figure 56 Creating an ALPA error graph

Managing performance graphs

This section provides the following procedures for managing performance graphs:

- Saving graphs to a canvas, page 137
- Adding a graph to an existing canvas, page 138
- Printing graphs, page 138
- Modifying an existing graph, page 139

Saving graphs to a canvas

Saving graphs is especially useful when you create customized graphs and do not want to re-create them every time you access the Performance Monitor module.

When you save graphs, you must save them to a canvas. The following procedure describes how to save graphs to a new canvas.

Saving graphs

1. Launch the Performance Monitor module as described on page 132.
2. Create basic or advanced Performance Monitor graphs, as described in "Creating a basic Performance Monitor graph" on page 132 and "Creating advanced Performance Monitor graphs" on page 134.

   The graphs are displayed in the in the Performance Monitor window.
3. Select **File > Save Current Canvas Configuration**.

   The Save Canvas Configuration dialog box opens.
4. Enter a name and description for the configuration and then click **Save Canvas**.

   A message confirms that the configuration was successfully saved to the switch.

Adding a graph to an existing canvas

The following procedure assumes that a canvas is already created.

To create a new canvas, you must first create graphs, as described in "Creating a basic Performance Monitor graph" on page 132 and "Creating advanced Performance Monitor graphs" on page 134, and then save those graphs to a canvas, as described in "Saving graphs to a canvas" on page 137.

Adding a graph

1. Select **File > Display Canvas Configurations**.

   The Canvas Configuration List is displayed. The message `No Canvas configuration to display` appears if there are no saved canvas configurations.
2. Click a canvas in the list.
3. Click **Edit**.

   The Edit Canvas dialog box opens.
4. Click **Add**.

   A list of graphs is displayed.
5. Click a graph to add it to the canvas.
6. Click **Save**.

Printing graphs

You can print a single graph or all the graphs displayed on the selected canvas configuration. Only one canvas configuration can be opened at a time.

Printing a single graph

1. Launch the Performance Monitor module as described on page 132.
2. Create a basic or advanced Performance Monitor graph as described in "Creating a basic Performance Monitor graph" on page 132 and "Creating advanced Performance Monitor graphs" on page 134.
3. Right-click anywhere in the graph and click **Print**.

   The print dialog box opens.
4. Click **OK**.

Printing all graphs in a canvas

1. Launch the Performance Monitor module as described on page 132.
2. Select **File > Display Canvas Configurations**.

   The Canvas Configuration List is displayed. The message `No Canvas configuration to display` appears if there are no saved canvas configurations.
3. Select a canvas from the list and click **Load**.

   The graphs from that canvas are displayed in the Performance Monitor window.

4. Select **File > Print All Graphs**.

   The print dialog box opens.

5. Click **OK**.

Modifying an existing graph

Use the following procedure to modify an existing graph that is saved in a canvas.

1. Launch the Performance Monitor module as described on page 132.
2. Select **File > Display Canvas Configurations**.

   The Canvas Configuration List is displayed. The message `No Canvas configuration to display` appears if there are no saved canvas configurations.

3. Select a canvas from the list and click **Edit**.

   The Performance Monitor Canvas: *Canvas Name* dialog box opens.

4. Select a graph from the list and click **Edit**.

NOTE: The Edit button is enabled only for the graphs that are configurable or editable.

5. Make changes in the Edit dialog box, as necessary.
6. Click **OK** to close the Edit dialog box.
7. Click **Save** to save the changes and close the Performance Monitor Canvas dialog box.
8. Click **Close** to close the Canvas Configuration List.

14 Limitations

This section provides the following information:

- General Advanced Web Tools limitations, page 141
- Platform-specific limitations, page 145
- Limitations when using the Mozilla browser, page 145

General Advanced Web Tools limitations

Table 14 lists general Advanced Web Tools limitations that apply to all browsers and switch platforms.

Table 14 Advanced Web Tools limitations

Problem area	Details
Browser	The Fabric Watch, Switch Admin, HA, Name Server, and Zone Admin modules are separate applets embedded in HTML pages. The successful launch of an applet depends on whether the browser can successfully load the HTML page. Occasionally, you will see a blank browser window with the message `loading pages...` that is stuck. This is likely caused by a sudden loss of the switch web server (either by normal HA failover, reboot, or other causes). **Workaround:** If the Fabric Watch, Switch Admin, HA, Name Server, or Zone Admin modules hang, close this window and relaunch the module.
Browser	An Advanced Web Tools browser window might stop responding following an HA failover immediately after a zoning configuration was enabled or disabled. It is likely that the web daemon was terminated by the HA failover before the HTTP request was sent back. **Workaround:** If one of the Advanced Web Tools modules is hanging, close the window and relaunch the module. If the module is locked, shut down and relaunch the Advanced Web Tools application.
Firmware download	There are multiple phases to firmware download and activation. When Advanced Web Tools reports that firmware download has completed successfully, this indicates that a basic sanity check, package retrieval, package unloading, and verification was successful. Advanced Web Tools forces a full package installation. A reboot is required to activate the newly downloaded firmware. This reboot is performed automatically. Although Advanced Web Tools screens continue to be visible during the reboot, they are not available. Wait approximately 10 minutes to ensure that all the application windows have been restored. If Advanced Web Tools fails to respond after 20 minutes, you might need to close all Advanced Web Tools applications windows and restart them or to contact your system administrator for network assistance. The Advanced Web Tools loss of network connectivity during a failover or reboot (initiated though the `firmwaredownload` command) varies for different configurations: • Core Switch 2/64, SAN Director 2/128, and 4/256 SAN Director: Loss of network connectivity is up to 5 minutes if the power-on self-test (POST) is disabled. If POST is enabled, the loss of network connectivity can exceed 5 minutes. • 4/8 SAN Switch, 4/16 SAN Switch, SAN Switch 2/8V, SAN Switch 2/16V, SAN Switch 2/32, 4Gb SAN Switch for HP p-Class BladeSystem, and SAN Switch 4/32: Loss of network connectivity is up to 1 minute if POST is disabled. If POST is enabled, the loss of network connectivity can exceed 1 minute.
HTTP timeout	Occasionally, you might see the following message when you try to get data from a switch or to send a request to the switch: `Failed to get switch response. Please verify the status of your last operation and try again if necessary.` This indicates that an HTTP request did not get a response. The request was sent to the switch, but the connection was down, probably caused by a temporary loss of the web server on the switch. Due to the nature of an HTTP connection, Advanced Web Tools reports this error after a 90-second default timeout. In this case, verify the status of your last request, using telnet to check related status, or click the **Refresh** button from the Advanced Web Tools application you were working on to retrieve related data. If your request did not get through to the switch, resubmit it. Executing a refresh from Advanced Web Tools retrieves a copy of switch data at that moment; the data you entered can be lost if it was not already committed to the switch.

Table 14 Advanced Web Tools limitations (continued)

Problem area	Details
Java Plug-in	When there is a dialog box opened for a module (for example, Switch Admin, Zone Admin, or Fabric Watch) and you try to open another module, the initial login dialog box receives an error and closes. This is a known defect in the Java 1.3.1_04 Plug-in and is documented in Bug Id 4763605 (available from www.java.sun.com). **Workaround:** Close and reopen the module.
Licenses	If you remove the Advanced Web Tools license after Advanced Web Tools application windows are opened, Advanced Web Tools displays the Web License Missing dialog box. From this point on, Advanced Web Tools behavior is undefined if you continue with other operations after removing the license. **Workaround:** Close and relaunch the browser.

Loss of Connection	Occasionally, you might see the following message when you try to retrieve data from the switch or send a request to the switch:
	`Switch Status Checking`
	`The switch is not currently accessible.`
	The dialog box title may vary, because it indicates which module is having the problem.
	This is caused by the loss of HTTP connection with the switch, due to a variety of possible problems. Advanced Web Tools tries to regain the connection. While Advanced Web Tools is trying to regain the connection, check if your Ethernet connection is still functioning. If the problem is not with the Ethernet connection, wait for Advanced Web Tools to recover the connection and display the following message:
	`You will have to resubmit your request after closing this message.`
	If the temporary switch connection loss is caused by switch hot code load, or other similar operation, the Switch Explorer you are currently running can be downloaded from a different firmware version than the new one. In this case, the following message is displayed:
	`Switch connection is restored. The firmware version you are running is not in sync with the version currently on switch. Close your browser and re-launch Webtools.`
	Close Switch Explorer and relaunch Advanced Web Tools to reopen the connection.

Performance Monitor	If the web browser crashes or the Performance Monitor license is lost while the Performance Monitor module is running, some of the Performance Monitor resources owned by Advanced Web Tools might not be cleaned up correctly. **Workaround:** You might need to use the CLI to manually delete these counters. For example, if you detect resources owned by Advanced Web Tools (using the `perfshoweemonitor` command), but you have verified that no Advanced Web Tools users are actually using them, use the `perfdeleemonitor` or `perfcleareemonitor` command to free the resources.
Performance Monitor	For SCSI Read, Write, or Read/Write on a LUN per Port graphs, Fabric OS 4.1.0 (and later 4.x versions) allows you to enable only two bytes or fewer for the LUN value mask setting. Fabric OS 3.1 (and later 3.x versions) allows up to three bytes. Advanced Web Tools displays an error message if you exceed this limit. **Workaround:** There is no workaround.

Table 14 Advanced Web Tools limitations (continued)

Problem area	Details
Refresh option in browsers	When a pop-up window requesting a user response is pushed into the background and a refresh is requested, a fatal Internet Explorer error may occur. **Workaround:** Restart the browser.
Refresh option in browsers	Advanced Web Tools must be restarted when the Ethernet IP address is changed using the `NetworkConfig View` command. Advanced Web Tools appears to hang if it is not restarted after this operation is executed. **Workaround:** Restart the browser.
Refresh option in browsers	If you change the switch name or domain ID using the CLI after the Advanced Web Tools Switch Admin module has started, the new switch name or domain ID is not updated on the header of the Switch Admin page. Clicking the Refresh button does not fix the problem. **Workaround:** Click the **Switch** tab and the Switch Admin header is updated.
Refresh option in browsers	If you change the switch name using the Advanced Web Tools Switch Admin page or SNMP and then open a telnet window to verify the name change, the CLI prompt (for example, `switch:admin>`) displays the previous name. The telnet prompt cannot pick up the new switch name until the switch is fastbooted. **Workaround:** To display the correct switch name in the CLI prompt after a switch name update using Advanced Web Tools or SNMP, fastboot the switch.
Refresh option in browsers	Following a switch enable or disable, you must wait at least 25–30 seconds for the fabric to reconfigure and for FSPF route calculations to complete before requesting routing information. If accessed too early, routing information is not shown. **Workaround:** Following a switch enable or disable, wait at least 25–30 seconds before further action.
Refresh option in browsers	The Advanced Web Tools Switch Explorer might continue to display a switch from the Switch View, even when the switch has been removed from the fabric. **Workaround:** If this behavior is seen, relaunch the Switch Explorer. If the switch was removed from the fabric, the Fabric View window lists the switch as unavailable.
Refresh option in browsers	In the Switch Admin module, Switch tab, if you click the Refresh button, you might not be able to click the data entry fields to enter text. This behavior occasionally happens on a notebook or laptop computer; it rarely happens on a desktop computer. **Workaround:** If this happens, restart the browser.
Switch Explorer closure	If upfront login is enabled, and the session times out or you log out or close the Switch Explorer window, all other windows belonging to the session are invalidated. After a short delay these windows become grayed out and unusable, but are not closed. You must manually close these windows.
Switch View	Occasionally, switches might display the port icons correctly, but be missing one or more control button icons. **Workaround:** Close the Switch View of the switch and reopen it.

Table 14 Advanced Web Tools limitations (continued)

Problem area	Details
Windows operating systems	Occasionally, you do not see the `Lost connection to the switch` message on the Switch View, even though the Ethernet connection has been lost. You might still be able to invoke various features from Switch View, such as Status, Fan Temp, Power, and Beacon. This problem might be seen in the Core Switch 2/64, for example, when you see the `Lost connection to the switch` error for a single switch in the chassis, when a lost connection affects both logical switches. **Workaround:** Verify Ethernet connection to the switch by pinging the logical switch IP address.
Zone Admin	The accessibility matrix in the Zone Admin module does not show hosts and devices zoned by QuickLoop AL_PA as being accessible to each other.

Platform-specific limitations

Table 15 lists Advanced Web Tools limitations that are specific to the Core Switch 2/64 and to the SAN Director 2/128 and 4/256 SAN Director when they are configured to have two domains.

Table 15 Platform-specific limitations

Problem area	Details
Switch View	Neither CP is updated in the Switch View (see Figure 3 on page 26) when switch 0 is being rebooted. The CP data displayed on this Switch View is dependent on switch 0, and that data is not available when switch 0 is rebooting. **Workaround:** Wait until the reboot is finished and Switch View polling occurs; the CPs are then updated properly.
Java Plug-in	The Java Plug-in might sometimes have problems focusing on a particular field in an open applet if you have the same window open for both logical switches. **Workaround:** When this problem occurs, close and relaunch the affected applet.

Limitations when using the Mozilla browser

Table 16 lists limitations in Advanced Web Tools that occur when you use the Mozilla browser on a Linux system. These limitations do not occur when using Internet Explorer on Windows systems.

Table 16 Advanced Web Tools limitations when using the Mozilla browser

Problem area	Details
Mozilla Browser on Red Hat operating system	On the Red Hat platform, the default system font size is larger than on other platforms. This can cause tabbed panes to not line up. There is no impact on functionality.
Mozilla Browser on Solaris operating system	On a Solaris/Mozilla browser, some pop-up windows (for example, the firmware download completion message and Performance Monitor dialog boxes) display in the background, behind other windows. This can give the appearance of a session hang. **Workaround:** If you are apparently locked out of other windows in the Solaris/Mozilla environment, look for a pop-up window that needs to be dismissed before proceeding further.

Table 16 Advanced Web Tools limitations when using the Mozilla browser (continued)

Problem area	Details
Performance Monitor module	When creating performance graphs, you might not be able to drag and drop port numbers or AL_PAs in the graph setup dialog box. **Workaround:** Enter the port numbers and AL_PAs in the appropriate fields.
Switch Admin, Routing tab	When you launch Advanced Web Tools and open the Switch Admin module for the first time, if you click the Routing tab, the FSPF route tree nodes do not display correctly. **Workaround:** Click another tab in the Switch Admin module; then select the **Routing** tab again.
Telnet	Mozilla browsers do not support the telnet application. **Workaround:** Launch an external telnet process.
Zone Admin	If you make changes in the Zone Admin module and then close the module without saving your changes, your changes are lost. If you have unsaved changes and you close the module by selecting File > Close, you receive a message warning that your changes are not saved and requesting confirmation before the module is closed. If you have unsaved changes and you close the module by clicking the X in the upper right corner of the window, you receive a warning message only if you are using Internet Explorer. If you are using the Mozilla browser, you do not receive this message and any unsaved changes are lost. **Workaround:** Always close the Zone Admin module by selecting File > Close. If you have not saved your changes, for all browsers, a warning message is displayed, requesting confirmation before the module is closed.

Index